PATENT OFFICE
JAPANESE COVERNMENT

This is to certify that the annexed is a true copy of the following application as filed with this Office.

Date of Application: March 26, 1998
Application Number : P10-79837
Applicant(s) : Nippon Telegraph & Telephone Corporation

February 5, 1999

Commissioner,
Patent Office Takeshi ISAYAMA

Number of Certificate: H 11-3003894

N-90

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: １９９８年　３月２６日

出願番号
Application Number: 平成１０年特許願第０７９８３７号

出願人
Applicant (s): 日本電信電話株式会社

１９９９年　２月　５日

特許庁長官
Commissioner,
Patent Office 伴佐山建志

出証番号　出証特平１１－３００３８９４

【書類名】　特許願

【整理番号】　NTTH097177

【提出日】　平成10年 3月26日

【あて先】　特許庁長官殿

【国際特許分類】　H04L　9/28

【発明の名称】　接続制御方法および通信網

【請求項の数】　4

【発明者】

【住所又は居所】　東京都新宿区西新宿三丁目１９番２号　日本電信電話株式会社内

【氏名】　久田　裕介

【発明者】

【住所又は居所】　東京都新宿区西新宿三丁目１９番２号　日本電信電話株式会社内

【氏名】　小野　諭

【発明者】

【住所又は居所】　東京都新宿区西新宿三丁目１９番２号　日本電信電話株式会社内

【氏名】　市川　晴久

【特許出願人】

【識別番号】　000004226

【氏名又は名称】　日本電信電話株式会社

【代表者】　宮津　純一郎

【代理人】

【識別番号】　100083806

【弁理士】

【氏名又は名称】　三好　秀和

【電話番号】　03-3504-3075

【選任した代理人】

【識別番号】　100068342

【弁理士】

【氏名又は名称】　三好　保男

【手数料の表示】

【予納台帳番号】　001982

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9701396

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　接続制御方法および通信網

【特許請求の範囲】

【請求項１】　通信網において着信者の前記通信網における識別子を隠蔽しつつ、前記通信網における識別子を隠蔽した他のユーザからの通信の接続を制御する接続制御方法であって、

通信網内の第１の機関がユーザに役割識別子を付与し、

第２の機関が役割識別子とユーザに関する情報とを対にして他のユーザから閲覧可能なように保持し、

発信者は前記役割識別子とユーザに関する情報とを対にした情報に基づいて着信者を役割識別子で指定し、

第３の機関は前記指定に基づいて前記発信者に対して発信者役割識別子、着信者役割識別子、発信者フラグ、移転制御フラグ、および有効期限を情報として含む個別化アクセスチケットを発行し、

第４の機関は発信者からの接続要求を、前記役割識別子、前記個別化アクセスチケット、および前記個別化アクセスチケットに対する電子署名の持つ情報を用いて、個別化アクセスチケットが改竄されていないこと、発信者役割識別子が個別化アクセスチケットに含まれていること、および個別化アクセスチケットが有効期限内であることの３要件をすべて検証し、検証結果がすべて正しい場合に限り、第４の機関が接続している通信網における物理的な接続制御方式に変換することで接続制御を行うこと

を特徴とする接続制御方法。

【請求項２】　前記個別化アクセスチケットに関する第４の機関の認証結果が正しくても、着信者が第４の機関の着信拒否リストにそのチケットを登録している場合は、第４の機関は当該接続要求を拒否することを特徴とする請求項１記載の接続制御方法。

【請求項３】　ユーザの通信網における識別子を隠蔽しつつ、通信網における識別子を隠蔽した他のユーザからの接続を制御可能とする通信網であって、

通信網内のユーザに役割識別子を付与する第１の機関と、

前記付与された役割識別子と該役割識別子に対応するユーザに関する情報とを対にして他のユーザから閲覧可能なように保持する第２の機関と、

通信網内の発信ユーザにより、他のユーザがその役割識別子によって着信先として指定された場合に、該役割識別子に基づいて前記発信ユーザに対して発信者匿名識別子、着信者匿名識別子、発信者フラグ、移転制御フラグ、および有効期限を情報として含む個別化アクセスチケットを発行する第３の機関と、

発信者からの接続要求を、前記役割識別子、前記個別化アクセスチケット、および前記個別化アクセスチケットに対する電子署名の持つ情報を用いて、個別化アクセスチケットが改竄されていないこと、発信者役割識別子が個別化アクセスチケットに含まれていること、および個別化アクセスチケットが有効期限内であることの３要件をすべて検証し、検証結果がすべて正しい場合に限り、通信網における物理的な接続制御方式に変換することで接続制御を行う第４の機関と

を有することを特徴とする通信網。

【請求項４】　前記第４の機関は、前記個別化アクセスチケットに関する第４の機関の認証結果が正しくても、着信者が第４の機関の着信拒否リストに該個別化アクセスチケットを登録している場合は、第４の機関は当該接続要求を拒否する拒否手段を有することを特徴とする請求項３記載の通信網。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、通信網において着信者の通信網における識別子を隠蔽しつつ、通信網における識別子を隠蔽した他のユーザからの通信の接続を制御する接続制御方法および通信網に関する。

【０００２】

【従来の技術】

近年、電話やコンピュータネットワークを用いた個人攻撃、例えば嫌がらせ、名誉毀損等が深刻な社会問題になっている。このような個人攻撃は通信網を介して氏名、性別、年齢、電話番号、電子メールアドレスといったプライバシー情報が第三者に漏洩するために発生するものである。具体的には、第三者による盗聴

、偽装等の盗難、第三者による意図的な収集（アンケート）、発信者の間違い電話等の端末操作ミス、発信者によるやむを得ない公開（情報誌、電子掲示板、ホームページ等）がある。

【０００３】

現在、盗難対策には認証、暗号化があり、間違い電話対策には端末の電話帳機能がある。また、第三者によるアンケート等の意図的な収集および発信者によるやむを得ない公開に対しては、いくつかの対策が実施されているが、いずれも漏洩を完全に防止することはできない。

【０００４】

求人（仲間募集）や売買のように他のユーザと個人的に連絡を取る必要があるユーザは、最低限、氏名と連絡先を情報誌、電子掲示板、またはホームページに掲載しなければならない。また、性別、年齢といったプライバシー情報を公開しなければならない場合もある。ところが、これらのメディアを閲覧するのは善意のユーザだけではない。個人攻撃を仕掛けようと企むユーザも閲覧する可能性は決して小さくない。そこで、情報を公開したユーザを何らかの手段で個人攻撃から保護することが必要になる。

【０００５】

このとき、そのユーザの取り得る戦略は２種類ある。ひとつは情報を限定公開する戦略で、具体的にはニックネームがある。もうひとつは接続相手を着信側で限定する戦略で、具体的には二重番号登録、発信者番号通知、着信拒否、匿名電子メール(Anonymous Mails) がある。

【０００６】

インターネットやパソコン通信の電子掲示板システムではニックネーム（ハンドルネーム）による発信が可能なため、実名を隠蔽することができる。しかしながら、善意のユーザにはすべてのプライバシー情報を公開するけれども、悪意のユーザには公開しないといったような制御はできないし、発信者の電子メールアドレスも隠蔽できない。このため、第三者から攻撃される恐れがある。

【０００７】

二重番号では、図２７に示すように、回線に複数の電話番号を割り当て、その

うちの一部の番号への呼をすべて自動的に切断するため、個人攻撃を被る恐れはない。その代わり、着呼可能な番号を知る者には厳重に守秘義務が課される。

【０００８】

また、発信者番号通知は、図２８に示すように、発信者電話番号を着信側端末に通知するものであり、アナログ公衆網、ＩＳＤＮ、デジタル携帯網で提供されているが、番号非通知の場合には、着信端末にも何も表示されない。

【０００９】

一方、着信拒否は、図２９に示すように、呼を自動的に切断する機能であり、アナログ公衆網、ＩＳＤＮ、デジタル携帯網で提供されている。仕様は網によって異なる。アナログ公衆網とＩＳＤＮでは、着信側回線あるいは端末で指定した発信者番号の呼以外は接続しない。逆に、デジタル携帯網では、着信側端末で設定した発信者番号の呼を切断する。

【００１０】

一般に、発信者番号通知と着信拒否は組み合わせて利用される。ところが、両者を組み合わせると、発信者と着信者のいずれか一方しか保護できなくなる。アナログ公衆網やＩＳＤＮでは番号非通知の呼を切断するため、番号漏洩を防止できなくなる。仕様を逆手にとると、個人情報の収集手段として利用できるからである。一方、デジタル携帯網では番号非通知の呼を切断しないため、着信者を個人攻撃から保護できなくなる。

【００１１】

匿名電子メールでは、図３０に示すように、発信者メールアドレスをリメーラ（remailer）機能を持つメールサーバのメールアドレスに書き換えて送信先に転送する。このように、発信者メールアドレスを隠蔽するため、発信者メールアドレスの漏洩を防ぐことができる。その一方で、匿名による攻撃が可能になるため、着信者が第三者から攻撃される危険性はより高くなる。

【００１２】

これを防ぐために、着信者から要求があった場合には、リメーラはその着信者宛の匿名メールの配信を中止する。ところが、この機能を用いると番号漏洩を防ぐことはできなくなる。着信拒否同様、個人情報の収集手段として利用できるか

らである。

【００１３】

【発明が解決しようとする課題】

上述したように、従来のニックネーム、二重番号登録、発信者番号通知、着信拒否、匿名電子メール等の方法では、それぞれ発信者の電子メールアドレスを隠蔽できず、第三者から攻撃されたり、着呼可能番号を知る者に厳重な守秘義務が課せられたり、番号非通知の呼を切断しない場合もあり、着信者を個人攻撃から保護できなかったり、匿名による攻撃が可能となり、着信者が第三者から攻撃される危険性が高くなるというような種々の問題がある。

【００１４】

本発明は、上記に鑑みてなされたもので、その目的とするところは、第三者による意図的な収集およびユーザによるやむを得ない公開に対して匿名性とセキュリティを確保すべく発信者および着信者の匿名性を保持しつつ発信者からの通信の接続を可能とし、着信者が匿名性を悪用した発信者による攻撃にさらされた場合には、その攻撃による着信者への被害を食い止めることを可能とする接続制御方法および通信網を提供することにある。

【００１５】

【課題を解決するための手段】

上記目的を達成するため、請求項１の本発明は、通信網において着信者の前記通信網における識別子を隠蔽しつつ、他のユーザからの前記通信網における識別子を隠蔽した通信の接続を制御する接続制御方法であって、通信網内の第１の機関がユーザに役割識別子を付与し、第２の機関が役割識別子とユーザに関する情報とを対にして他のユーザから閲覧可能なように保持し、発信者は前記役割識別子とユーザに関する情報とを対にした情報に基づいて着信者を役割識別子で指定し、第３の機関は前記指定に基づいて前記発信者に対して発信者匿名識別子、着信者匿名識別子、発信者フラグ、移転制御フラグ、および有効期限を情報として含む個別化アクセスチケットを発行し、第４の機関は発信者からの接続要求を、前記役割識別子、前記個別化アクセスチケット、および前記個別化アクセスチケットに対する電子署名の持つ情報を用いて、個別化アクセスチケットが改竄され

ていないこと、発信者役割識別子が個別化アクセスチケットに含まれていること、および個別化アクセスチケットが有効期限内であることの３要件をすべて検証し、検証結果がすべて正しい場合に限り、第４の機関が接続している通信網における物理的な接続制御方式に変換することで接続制御を行うことを要旨とする。

【００１６】

請求項１記載の本発明にあっては、ユーザに役割識別子を付与し、役割識別子とユーザに関する情報とを対にして他のユーザから閲覧可能に保持し、発信者は役割識別子とユーザに関する情報に基づいて着信者を役割識別子で指定し、この指定に基づいて発信者に対して発信者匿名識別子、着信者匿名識別子、発信者フラグ、移転制御フラグ、および、有効期限を含む個別化アクセスチケットを発行し、役割識別子および個別化アクセスチケットを用いて、個別化アクセスチケットに改竄がなく、発信者役割識別子が個別化アクセスチケットに含まれ、および個別化アクセスチケットが有効期限内であるという３要件をすべて検証し、検証結果がすべて正しい場合に発信者からの接続要求を通信網の物理的な接続制御方式に変換する接続制御を行う。

【００１７】

また、請求項２記載の本発明は、請求項１記載の発明において、前記個別化アクセスチケットに関する第４の機関の認証結果が正しくても、着信者が第４の機関の着信拒否リストにそのチケットを登録している場合は、第４の機関は当該接続要求を拒否することを要旨とする。

【００１８】

請求項２記載の本発明にあっては、個別化アクセスチケットに関する認証結果が正しくても、着信者の個別化アクセスチケットが着信拒否リストに登録している場合は、接続要求を拒否する。

【００１９】

更に、請求項３記載の本発明は、ユーザの通信網における識別子を隠蔽しつつ、他のユーザからの接続を制御可能とする通信網であって、通信網内のユーザに役割識別子を付与する第１の機関と、前記付与された役割識別子と該役割識別子に対応するユーザに関する情報とを対にして他のユーザから閲覧可能なように保

持する第２の機関と、通信網内の発信ユーザより、他のユーザがその役割識別子によって着信先として指定された場合に、該役割識別子に基づいて前記発信ユーザに対して発信者匿名識別子、着信者匿名識別子、発信者フラグ、移転制御フラグ、および有効期限を情報として含む個別化アクセスチケットを発行する第３の機関と、発信者からの接続要求を、前記役割識別子、前記個別化アクセスチケット、および前記個別化アクセスチケットに対する電子署名の持つ情報を用いて、該個別化アクセスチケットが改竄されていないこと、発信者役割識別子が個別化アクセスチケットに含まれていること、および個別化アクセスチケットが有効期限内であることの３要件をすべて検証し、検証結果がすべて正しい場合に限り、通信網における物理的な接続制御方式に変換することで接続制御を行う第４の機関とを有することを要旨とする。

【００２０】

請求項３記載の本発明にあっては、ユーザに役割識別子を付与し、役割識別子とユーザに関する情報とを対にして他のユーザから閲覧可能に保持し、発信者は役割識別子とユーザに関する情報に基づいて着信者を役割識別子で指定し、この指定に基づいて発信者に対して発信者役割識別子、着信者役割識別子、発信者フラグ、移転制御フラグ、および有効期限を情報として含む個別化アクセスチケットを発行し、役割識別子、個別化アクセスチケットおよび個別化アクセスチケットに対する電子署名を用いて、個別化アクセスチケットが改竄されていなくて、発信者役割識別子が個別化アクセスチケットに含まれ、および個別化アクセスチケットが有効期限内であるという３要件をすべて検証し、検証結果がすべて正しい場合に発信者からの接続要求を通信網の物理的な接続制御方式に変換する接続制御を行う。

【００２１】

請求項４記載の本発明は、請求項３記載の発明において、前記第４の機関が、前記個別化アクセスチケットに関する第４の機関の認証結果が正しくても、着信者が第４の機関の着信拒否リストに該個別化アクセスチケットを登録している場合は、第４の機関は当該接続要求を拒否する拒否手段を有することを要旨とする。

【００２２】

請求項４記載の本発明にあっては、個別化アクセスチケットに関する認証結果が正しくても、着信者の個別化アクセスチケットが着信拒否リストに登録している場合は、接続要求を拒否する。

【００２３】

【発明の実施の形態】

以下、図面を用いて本発明の実施の形態について説明する。本発明の接続制御方法は、通信網における発信者および着信者の匿名性を保持しつつ、発信者からの通信をも適宜可能とするものであり、基本的には着信者の本当の識別子を隠蔽した状態で、着信者の特性を表す情報のみを公開し、この公開された情報に基づいて、匿名性を保持したまま通信を希望する者に対して限定的なアクセス権を付与することにある。

【００２４】

具体的には、図１（ａ）に示すように、ユーザに対して個人情報を隠蔽した役割識別子（Anonymous Identification：ＡＩＤと略称する）を付与し、この役割識別子ＡＩＤをユーザの特性を表す情報である趣味、年齢、職業等のようなユーザをネットワーク上で特定はできないが、発信者にとって当該ユーザと通信する価値があるかどうかを判断するための有用な情報と組にしてネットワークに公開する。

【００２５】

また、発信者は、前記公開された情報を閲覧または検索することにより自分が通信したい相手を捜すことができる。すなわち、発信者が発信者自身の匿名性を保持したままある相手と通信したい場合には、その相手の役割識別子を指定し、個別化アクセスチケットＰＡＴ（Personalized Access Ticket）を取得する。

【００２６】

個別化アクセスチケットＰＡＴには、発信者、着信者それぞれの役割識別子ＡＩＤの他に、発信者フラグ、移転制御フラグ、および、有効期限の各情報が記載されている。移転制御フラグは、図１（ｂ），（ｃ）に示すように着信拒否等の接続制御を行うために使用される。すなわち、移転制御フラグを立てると、後述

するセキュア・コミュニケーション・サービスＳＣＳ（Secure Communication Service）は、接続要求の際に、発信者に対し、例えば署名の検証、パスワード要求等の認証を行う。また、移転制御フラグを立てない場合には、セキュア・コミュニケーション・サービスＳＣＳは認証無しで接続要求をセキュア・コミュニケーション・サービスＳＣＳが接続している物理的通信網に渡す。すなわち、移転制御は役割識別子ＡＩＤがこれを認証局ＣＡ(Certification Authority) から割り当てられたユーザによって正当に利用されているかを認証するために用いられる。

【００２７】

本発明の接続制御方法を実施する通信網においては、ユーザに対する役割識別子ＡＩＤの付与、役割識別子ＡＩＤと組み合わされた情報の保持、個別化アクセスチケットＰＡＴの発行、および個別化アクセスチケットＰＡＴに基づく接続制御はそれぞれ別の機関で行われている。これは、それぞれの行為に関して保持すべきセキュリティレベルに差があるので、別々の機関で実行した方がネットワーク全体のセキュリティの保持には好都合だからである。

【００２８】

図２は、本発明の一実施形態の全体構成図である。本実施形態はインターネット電子メールシステムを対象としたものである。図２において、１は認証局ＣＡであり、認証権限と役割識別子ＡＩＤの発行権限を有し、ユーザに対して役割識別子を割り当てる機能を有する。３はユーザであり、５はセキュア・コミュニケーション・サービスＳＣＳであり、ユーザ３間の電子メールを転送し、必要に応じて着信拒否および個人識別子の同一性を判定し、取り出す。７はアノニマス・ディレクトリ・サービスＡＤＳであり、役割識別子ＡＩＤ、移転制御情報、有効期限、および、プライバシー情報を管理するデータベースである。すなわち、アノニマス・ディレクトリ・サービスＡＤＳ７は、検索者の役割識別子ＡＩＤと検索条件（一般に、プライバシー情報）にマッチした登録者の役割識別子ＡＩＤから個別化アクセスチケットＰＡＴを発行し、検索者に交付する機能を有する。

【００２９】

まず、ユーザの要求に基づいて個人識別子から役割識別子ＡＩＤを生成し、そ

のユーザに割り当てるまでの一連の処理について説明する。

【００３０】

図３は、個人識別子ＯＩＤ(Official Identification) と役割識別子ＡＩＤの例を示している。同図に示すように、個人識別子ＯＩＤは、図３（ａ）に示すように認証局ＣＡ１がユーザに一意に生成した任意の文字列に対して認証局ＣＡ１が秘密鍵で電子署名したものである。また、役割識別子ＡＩＤは、図３（ｂ）に示すように個人識別子ＯＩＤの一部とその位置情報、冗長な文字列、ＳＣＳのホストＯＩＤからなる文字列に対し、認証局ＣＡ１の秘密鍵で電子署名を施したものである。

【００３１】

次に、ユーザ３が役割識別子ＡＩＤを認証局ＣＡ１に対して請求する処理について図４に示すフローチャートを参照して説明する。ユーザは個人識別子ＯＩＤと請求項目を入力して（ステップＳ４１１）、図７に示すようにＡＩＤ請求メッセージを作成し（ステップＳ４１３）、ユーザＯＩＤの秘密鍵で署名、暗号化し（ステップＳ４１５）、それから該ＡＩＤ請求メッセージを認証局ＣＡ１に電子メールで送信する（ステップＳ１４７）。

【００３２】

ＡＩＤ請求メッセージは、発信者の個人識別子ＯＩＤと請求項目から構成され、請求項目は次に示す２種類のうちのいずれかである。

(1) 新規な役割識別子ＡＩＤの割り当てを要求する場合：

REQUEST AID ＜要求するＡＩＤの数＞

(2) 既存の役割識別子ＡＩＤの廃止を要求する場合：

DISCARD AID ＜廃止したいＡＩＤの実体＞

【００３３】

次に、上述した役割識別子ＡＩＤの請求に対する認証局ＣＡ１が役割識別子ＡＩＤをユーザ３に対して交付する処理について図５に示すフローチャートを参照して説明する。図５において、認証局ＣＡ１は、ユーザ３からの上述したＡＩＤ請求メッセージを受信すると（ステップＳ５１１）、認証局ＣＡ１はユーザ３のＯＩＤ公開鍵を用いてＡＩＤ請求メッセージ（図７）を復号化、認証する（ステ

ップＳ５１３）。認証局ＣＡ１は該メッセージが改竄されているか否かをチェックする（ステップＳ５１５）。改竄を検出した場合には、該メッセージを破棄するが、改竄が認められなかった場合には、認証局ＣＡ１は役割識別子ＡＩＤを生成し（ステップＳ５１７）、ＡＩＤ秘密鍵およびＡＩＤ公開鍵を生成し（ステップＳ５１９）、図８に示すＡＩＤ交付メッセージを生成する（ステップＳ５２１）。それから、認証局ＣＡ１は該メッセージをユーザＯＩＤの公開鍵で署名、暗号化し（ステップＳ５２３）、この署名したメッセージをユーザ３のＯＩＤに送信する（ステップＳ５２５）。

【００３４】

次に、図６に示すフローチャートを参照して、ユーザにおけるＡＩＤ交付処理について説明する。図６において、ユーザ３が認証局ＣＡ１からの暗号化されたＡＩＤ交付メッセージを受信すると（ステップＳ６１１）、ユーザ３はユーザ秘密鍵を用いてＡＩＤ交付メッセージを復号化、認証し（ステップＳ６１３）、該メッセージが改竄されているか否かをチェックする（ステップＳ６１５）。改竄を検出した場合には、エラーメッセージを出力し、該ＡＩＤ交付メッセージを破棄する（ステップＳ６１７）。また、改竄が認められない場合には、ＡＩＤ交付メッセージから役割識別子ＡＩＤとＡＩＤ秘密鍵を抽出し、ユーザ３に通知する（ステップＳ６１９）。

【００３５】

ＡＩＤ交付メッセージは、図８に示すように発信者ＯＩＤと処理結果から構成されている。処理結果は次に示す２種類のうちのいずれかである。

(1) 新規な役割識別子ＡＩＤの交付の場合：

NEW AID ＜新規ＡＩＤの実体とＡＩＤの秘密鍵｜ＡＩＤ取得失敗＞

(2) 既存の役割識別子ＡＩＤの廃止

DISCARD AID ＜既存ＡＩＤの実体＞＜廃止完了｜廃止失敗＞

【００３６】

次に、認証局ＣＡにおける役割識別子ＡＩＤの生成処理について図９、図１０を参照して説明する。図９において、認証局ＣＡ１は乱数発生等の任意の手段を用いて、個人識別子ＯＩＤの全長Ｌと等しい長さの文字列を生成し、この文字列

を仮の役割識別子ＡＩＤとして生成する（ステップＳ９１１）。

【００３７】

次に、個人識別子ＯＩＤの複写を行うために、個人識別子ＯＩＤのコピー範囲を指定するｐとｌの値を決定する（ステップＳ９１３）。これは、乱数発生等の任意の手段を用いて、パラメータp_iとl_iの値をそれぞれ$0 \leqq p_i \leqq L$および$l_{min} \leqq l_i \leqq l_{Max}$のようにコピー範囲を決定する。ここで、Ｌは個人識別子ＯＩＤの全長であり、l_{min}およびl_{Max}は$0 < l_{min} < l_{Max} < L$が成り立つ範囲で任意に定めた値とする。それから、コピー先頭位置を個人識別子ＯＩＤの先頭から距離p_iに設定し、終端位置を$p_i + l_i$に設定するというようにコピー範囲を設定する。次に、図１０（ａ），（ｂ）に示すように、ペースト先頭位置を仮の役割識別子ＡＩＤの先頭から距離p_iに設定し、終端位置を$p_i + l_i$に設定するというようにペースト位置を設定する。

【００３８】

それから、図１０（ａ），（ｂ）に示すように、上述したコピー範囲の文字列を仮の役割識別子ＡＩＤの上述したペースト位置に上書きして複写する（ステップＳ９１５）。このように上書きした文字列の特定の位置に位置情報p_iおよびl_iの値を、ＣＡが定めた方法で暗号化して、図１０（ｃ）で指定した位置に付加し（ステップＳ９１７）、更にこの位置情報を付加した文字列にセキュア・コミュニケーション・サービスＳＣＳのホストＯＩＤ（ホスト名、ドメイン名、またはＩＰアドレス）を図１０（ｃ）に示すように付加する（ステップＳ９１９）。そして、このようにセキュア・コミュニケーション・サービスＳＣＳのホストＯＩＤを付加した文字列に認証局ＣＡのＯＩＤ秘密鍵で電子署名を施す（ステップＳ９２１）。

【００３９】

次に、役割識別子ＡＩＤによる個人情報の登録および検索について説明する。アノニマス・ディレクトリ・サービスＡＤＳ７において、個人情報を登録するまでの流れを図１１（ａ）に示す。同図に示すように、登録者であるユーザＢ３は自らの役割識別子ＡＩＤ、移転制御情報、有効期限、および、性別、年齢、趣味等のプライバシー情報をアノニマス・ディレクトリ・サービスＡＤＳ７に送付す

る。

【００４０】

また、アノニマス・ディレクトリ・サービスＡＤＳ７における検索処理を図１１（ｂ）に示す。検索者であるユーザＡ３は、自らの役割識別子ＡＩＤと例えば性別、年齢、趣味といったプライバシー情報からなる検索条件をアノニマス・ディレクトリ・サービスＡＤＳ７に送信する。アノニマス・ディレクトリ・サービスＡＤＳ７は、これらの情報を受信すると、検索条件にマッチした登録者の役割識別子ＡＩＤを抽出する。アノニマス・ディレクトリ・サービスＡＤＳ７は最後に検索者の役割識別子ＡＩＤと検索条件にマッチした登録者の役割識別子ＡＩＤから個別化アクセスチケットＰＡＴを生成し、検索者であるユーザＡ３に交付する。

【００４１】

個別化アクセスチケットの生成は、アノニマス・ディレクトリ・サービスＡＤＳ７の検索結果として生成する。

【００４２】

次に、図１２のフローチャートを参照して、ＡＤＳにおけるＰＡＴ生成処理について説明する。

【００４３】

１．検索者ＡＩＤ秘密鍵で署名された検索者ＡＩＤを入力する（ステップＳ１２１０）。

【００４４】

２．ステップＳ１２１０における検索者ＡＩＤをその検索者ＡＩＤの公開鍵で認証する（ステップＳ１２１１）。

【００４５】

３．ステップＳ１２１１における認証の結果

・検索者ＡＩＤが改竄されている場合処理を中止する。

・検索者ＡＩＤが改竄されていない場合、ステップＳ１２１５に進む。

【００４６】

４．ステップＳ１２１１で認証済みの検索者ＡＩＤを、登録者ＡＩＤ（ＡＤＳ登

録時に登録者ＡＩＤの秘密鍵で認証済み）と連結する（ステップＳ１２１５）。

【００４７】

５．ステップＳ１２１５で連結した、検索者ＡＩＤと登録者ＡＩＤからなる文字列に、登録者によりあらかじめ設定された移動制御フラグと有効期限を設定する。また、発信者フラグを「０」と設定する（ステップＳ１２１７）。

【００４８】

６．ステップＳ１２１７の結果に、ＡＤＳのＯＩＤ秘密鍵で署名する（ステップＳ１２１９）。

【００４９】

７．ステップＳ１２１９の結果（つまり、ＰＡＴ）を、検索者ＡＩＤに送信する（ステップＳ１２２１）。

【００５０】

なお、ＰＡＴを受信した検索者は、ＡＤＳのＯＩＤ公開鍵を用いて受信したＰＡＴを認証し、改竄されていなければ、これを検索者端末の記憶装置に記憶し、改竄されていれば、破棄します。この手順は、図６と同様である。

【００５１】

次に、個別化アクセスチケットＰＡＴによる移転制御について説明する。移転制御は、発信者番号通知のために行われるが、この発信者番号通知とは、着信者が発信者の役割識別子ＡＩＤと実際の発信者を対応付けられるようにすることである。

【００５２】

アノニマス・ディレクトリ・サービスＡＤＳ７および着信者は、個別化アクセスチケットＰＡＴの移転制御フラグを設定することにより、発信者に番号通知させるか否かを選択させることができる。

【００５３】

移転制御フラグを「１」に設定した場合には、セキュア・コミュニケーション・サービスＳＣＳ５で移転制御が行われるため、着信者は発信者の役割識別子ＡＩＤと実際の発信者を対応付けることができる（発信者番号通知）。また、移転制御フラグを「０」に設定した場合には、着信者は発信者の役割識別子ＡＩＤと

実際の発信者を対応付けることができない（発信者番号非通知）。

【００５４】

図１４のフローチャートを参照して、ＳＣＳにおけるメール接続制御の処理手順について説明する。

【００５５】

１．メールを入力する（ステップＳ１４１１）。

【００５６】

２．ステップＳ１４１１のメールのＴｏ：フィールドからＰＡＴを抽出する。次に、このＰＡＴに対するＡＤＳ公開鍵をＡＤＳに何らかの手段で問い合わせ、そのＡＤＳ公開鍵を取得する。そして、ＰＡＴをＡＤＳ公開鍵で認証する（ステップＳ１４１３）。

【００５７】

３．ステップＳ１４１３における認証の結果

・ＰＡＴが改竄されている場合、ステップＳ１４１１のメールを、メールのＦｒｏｍ：フィールドに記述された発信者ＡＩＤ宛に返信して、処理を中止する（ステップＳ１４２９）。

・ＰＡＴが改竄されていない場合、ステップＳ１４１７に進む。

【００５８】

４．ステップＳ１４１１のメールのＦｒｏｍ：フィールドから発信者ＡＩＤを抽出する。また、メールのＴｏ：フィールドのＰＡＴの移転制御フラグを解析し、ＰＡＴから発信者ＡＩＤを抽出する（ステップＳ１４１７，Ｓ１４１９）。

【００５９】

５．ステップＳ１４１７，Ｓ１４１９で抽出した発信者ＡＩＤ同士を比較する（ステップＳ１４２１）。

【００６０】

６．ステップＳ１４２１における比較の結果

・両者が一致しない場合ステップＳ１４１１のメールを、メールのＦｒｏｍ：フィールドに記述された発信者ＡＩＤ宛に返信して、処理を中止する（ステップＳ１４２９）。

・両者が一致する場合、ステップＳ１４２５に進む。

【００６１】

７．ステップＳ１４１１のメールのＴｏ：フィールドのＰＡＴから有効期限を抽出する（ステップＳ１４２５）。

【００６２】

８．ステップＳ１４１１のメールのＴｏ：フィールドのＰＡＴが有効期限内かどうかを検証する。

【００６３】

９．ステップＳ１４２１における検証の結果

・有効期限を過ぎている場合、ステップＳ１４１１のメールを、メールのＦｒｏｍ：フィールドに記述された発信者ＡＩＤ宛に返信して、処理を中止する（ステップＳ１４２９）。

・有効期限内の場合、ステップＳ１４３１に進む。

【００６４】

１０．ステップＳ１４１１のメールのＴｏ：フィールドのＰＡＴから移転制御フラグ値を調べる。

【００６５】

１１．ステップＳ１４１１のメールのＴｏ：フィールドのＰＡＴから移転制御フラグ値を抽出する（ステップＳ１４３１）。

【００６６】

１２．ステップＳ１４３１における抽出の結果

・移転制御フラグ値が「１」の場合、図１５～図１７の手順に従い、移転制御を行ってから（ステップＳ１４３５）、図１８の手順に従い、メールを着信者ＡＩＤ宛に転送する（ステップＳ１４３７）。

・移転制御フラグ値が「０」の場合、図１８の手順に従い、メールを着信者ＡＩＤ宛に転送する（ステップＳ１４３７）。

【００６７】

この移転制御について図１５～図１７を参照して説明する。まず、図１５において、セキュア・コミュニケーション・サービスＳＣＳ５は、個別化アクセスチ

ケットＰＡＴを入力すると（ステップＳ１５１１）、それから、セキュア・コミュニケーション・サービスＳＣＳ５は、任意の文字列、例えばタイムスタンプを生成し（ステップＳ１５１７）、この生成した文字列を発信者の役割識別子ＡＩＤに送信する（ステップＳ１５１９）。

【００６８】

ユーザにおいては、図１６に示すように、前記文字列を受信すると（ステップＳ１６１１）、この文字列に発信者役割識別子ＡＩＤの秘密鍵で署名し（ステップＳ１６１３）、署名つき該文字列をセキュア・コミュニケーション・サービスＳＣＳ５に送信する（ステップＳ１６１５）。

【００６９】

セキュア・コミュニケーション・サービスＳＣＳ５においては、図１７に示すように、署名つき前記文字列を受信すると（ステップＳ１７１１）、発信者の役割識別子ＡＩＤの公開鍵で認証し（ステップＳ１７１３）、改竄されているか否かをチェックする（ステップＳ１７１５）。改竄されている場合には、改竄されている旨を何らかの手段で発信者ＡＩＤに通知してからアボート（異常終了）するが（ステップＳ１７１７）、改竄されていない場合には、セキュア・コミュニケーション・サービスＳＣＳ５は、図１８に示す接続制御を行う。

【００７０】

以下、図１８のフローチャートを参照して接続制御について説明する。

【００７１】

１．メールのＴｏ：フィールドのＰＡＴから、発信者のＳＣＳホストＯＩＤと着信者のＳＣＳホストＯＩＤを抽出する（ステップＳ１８１１）。

【００７２】

２．ステップＳ１８１１で抽出した発信者、着信者それぞれのＳＣＳホストＯＩＤのデータ形式を調べる（ステップＳ１８１３）。

【００７３】

３．ステップＳ１８１３における調査の結果

・発信者ＳＣＳホストＯＩＤと着信者ＳＣＳホストＯＩＤのうち、少なくとも一方がホスト名もしくはドメイン名で与えられている場合には、ステップＳ１８

１５に進み、ホスト名またはドメイン名で与えられているＳＣＳホストＯＩＤをＤＮＳ(Domain Name Service) に問い合わせ、そのホスト名またはドメイン名に対するＩＰアドレスを取得してから、ステップＳ１８１７に進む。

・発信者ＳＣＳホストＯＩＤと着信者ＳＣＳホストＯＩＤがともにＩＰアドレスで与えられている場合には、そのままステップＳ１８１７に進む。

【００７４】

４．ステップＳ１８１５，Ｓ１８１７で抽出あるいは変換したＩＰアドレスを比較する（ステップＳ１８１７）。

【００７５】

５．ステップＳ１８１７における比較の結果

・発信者ＳＣＳホストＯＩＤ（ＩＰアドレス）と着信者ＳＣＳホストＯＩＤ（ＩＰアドレス）が一致する場合、ステップＳ１８１９からステップＳ１８２３に進み、発信者ＡＩＤをアカウントに持つＳＣＳホスト上で、着信者ＡＩＤを検索する（ステップＳ１８２３）。この検索の結果、着信者ＡＩＤのアカウントが、発信者ＡＩＤをアカウントに持つＳＣＳホスト上に存在しない場合、ステップＳ１８２５からステップＳ１８２７に進み、ステップＳ１８１１のメールを、メールのＦｒｏｍ：フィールドに記述された発信者ＡＩＤ宛に返信して、処理を中止する。

【００７６】

また、ステップＳ１８２５において、着信者ＡＩＤのアカウントが、発信者ＡＩＤをアカウントに持つＳＣＳホスト上に存在する場合、着信者ＡＩＤを検索条件として、着信拒否データベースに問い合わせる（ステップＳ１８２９）。

【００７７】

この問い合わせの結果、メールのＴｏ：フィールドのＰＡＴ、または、発信者ＡＩＤに含まれるＳＣＳホストＯＩＤが着信拒否データベースに登録されている場合、ステップＳ１８３１からステップＳ１８２７に進み、メールを、メールのＦｒｏｍ：フィールドに記述された発信者ＡＩＤ宛に返信して、処理を中止する。

【００７８】

また、ステップＳ１８３１において、メールのＴｏ：フィールドのＰＡＴ、または、発信者ＡＩＤに含まれるＳＣＳホストＯＩＤが着信拒否データベースに登録されていない場合、メールを、着信者のメールボックスまたはスプールに格納して正常終了する（ステップＳ１８３３）。

【００７９】

一方、ステップＳ１８１９において、発信者ＳＣＳホストＯＩＤ（ＩＰアドレス）と着信者ＳＣＳホストＯＩＤ（ＩＰアドレス）が一致しない場合、について説明する。

【００８０】

まず、ＳＭＴＰに従い、メールを着信者ＡＩＤをアカウントに持つＳＣＳホストに転送する（ステップＳ１８３５）。

【００８１】

次に、着信者ＡＩＤをアカウントに持つＳＣＳホスト上で、着信者ＡＩＤを検索する（ステップＳ１８３７）。

【００８２】

この検索の結果、着信者ＡＩＤのアカウントが、発信者ＡＩＤをアカウントに持つＳＣＳホスト上に存在しない場合、ステップＳ１８３９からステップＳ１８４１に進み、メールを、メールのＦｒｏｍ：フィールドに記述された発信者ＡＩＤ宛に返信して、処理を中止する。

【００８３】

また、ステップＳ１８３９において、着信者ＡＩＤのアカウントが、発信者ＡＩＤをアカウントに持つＳＣＳホスト上に存在する場合、ステップＳ１８４３に進む。ステップＳ１８４３では着信者ＡＩＤを検索条件として、着信拒否データベースに問い合わせる。

【００８４】

ステップＳ１８４３における問い合わせの結果、メールのＴｏ：フィールドのＰＡＴ、または、発信者ＡＩＤに含まれるＳＣＳホストＯＩＤが着信拒否データベースに登録されている場合、ステップＳ１８４５からステップＳ１８４１に進

み、メールを、メールのＦｒｏｍ：フィールドに記述された発信者ＡＩＤ宛に返信して、処理を中止する。

【００８５】

また、ステップＳ１８４５において、メールのＴｏ：フィールドのＰＡＴ、または、発信者ＡＩＤに含まれるＳＣＳホストＯＩＤが着信拒否データベースに登録されていない場合、ステップＳ１８４７に進み、メールを、着信者のメールボックスまたはスプールに格納して正常終了する。

【００８６】

図１９のフローチャートを参照して、ＳＣＳにおけるメール返信処理についてに説明する。

【００８７】

１．エラーを検出したＳＣＳホストは、ＰＡＴ＜エラーを検出したＳＣＳホストＯＩＤ｜Ｆｒｏｍ：フィールドの発信者ＡＩＤ＞を生成する（ステップＳ１９１１）。

【００８８】

２．ステップＳ１９１１のＳＣＳホストは、ステップＳ１９１１で生成したＰＡＴを、エラーが発生したメールのＴｏ：フィールドにセットする（ステップＳ１９１３）。

【００８９】

３．ステップＳ１９１１のＳＣＳホストは、ステップＳ１９１３でセットしたメールを（発信者ＡＩＤ宛に）送信する（ステップＳ１９１５）。

【００９０】

次に、個別化アクセスチケットＰＡＴに対する着信拒否について説明する。

【００９１】

着信者ＡＩＤ側で指定した個別化アクセスチケットＰＡＴがＴｏ：フィールドに記述されたメールが、着信者ＡＩＤに含まれるホストＯＩＤのセキュア・コミュニケーション・サービスＳＣＳ５に到着した場合には、そのセキュア・コミュニケーション・サービスＳＣＳ５はそのメールを着信者のメールボックスまたはスプールには格納せず、発信者ＡＩＤ宛に返信する。この一連の処理を着信拒否

と呼ぶ。

【００９２】

ユーザにおける着信拒否申請処理について図２２に示すフローチャートを参照して説明する。ユーザは役割識別子ＡＩＤと個別化アクセスチケットＰＡＴを入力し（ステップＳ２２１１）、図２４の上側に示す着信拒否申請メッセージを作成し（ステップＳ２２１３）、着信者ＡＩＤの秘密鍵で署名、暗号化する（ステップＳ２２１５）。それから、着信者はこの暗号化した申請メッセージをセキュア・コミュニケーション・サービスＳＣＳ５に送信する（ステップＳ２２１７）。

【００９３】

着信拒否申請メッセージは、図２４の上側に示すように、着信者の役割識別子ＡＩＤと申請項目から構成される。申請項目は次の２種類のうちのいずれかである。

(1) 着信拒否の設定

＜着信者ＡＩＤの実体＞REFUSE＜ＰＡＴの実体、ＩＰアドレス、ドメイン名、ホスト名＞

(2) 着信拒否の解除

＜着信者ＡＩＤの実体＞RECONNECT ＜ＰＡＴの実体、ＩＰアドレス、ドメイン名、ホスト名＞

【００９４】

次に、図２３に示すフローチャートを参照して、セキュア・コミュニケーション・サービスＳＣＳ５における着信拒否設定処理について説明する。セキュア・コミュニケーション・サービスＳＣＳ５は、着信拒否申請メッセージを受け取ると（ステップＳ２３１１）、着信者のＡＩＤ公開鍵で認証し（ステップＳ２３１３）、改竄されているか否かをチェックする（ステップＳ２３１５）。改竄されていない場合には、着信拒否メッセージから個別化アクセスチケットＰＡＴ、ＩＰアドレス、ドメイン名、またはホスト名を抽出し、該個別化アクセスチケットＰＡＴ、該ＩＰアドレス、該ドメイン名、該ホスト名を着信拒否データベース（ＤＢ）に登録（または削除）する（ステップＳ２３１７）。それから、図２４の

下側に示すような着信拒否通知メッセージを生成し（ステップＳ２３１９）、着信者ＡＩＤ公開鍵で署名、暗号化し（ステップＳ２３２１）、この暗号化されたメッセージを着信者ＡＩＤに返信する（ステップＳ２３２３）。

【００９５】

着信拒否通知メッセージは、図２４の下側に示すように、着信者の役割識別子ＡＩＤと処理結果から構成されている。処理結果は次に示す２種類のうちのいずれかである。

(1) 着信拒否の設定結果

＜着信者ＡＩＤの実体＞REFUSE＜成功｜失敗＞＜ＰＡＴの実体、ＩＰアドレス、ドメイン名、ホスト名＞

(2) 着信拒否の解除結果

＜着信者ＡＩＤの実体＞RECONNECT ＜成功｜失敗＞＜ＰＡＴの実体、ＩＰアドレス、ドメイン名、ホスト名＞

【００９６】

着信拒否の実行に当たっては、セキュア・コミュニケーション・サービスＳＣＳ５は、個別化アクセスチケットＰＡＴを着信拒否データベースに問い合わせる。該当個別化アクセスチケットが存在する場合、または、発信者ＡＩＤに、該当するＩＰアドレス、ホスト名、ドメイン名が含まれる場合には、メールを発信者ＡＩＤに返信する。存在しない場合には、メッセージを着信者アカウントのメールボックスまたはスプールに格納する。

【００９７】

図２５のフローチャートを参照して、同一性の判定について説明する。

【００９８】

１．変数$ＯＩＤ_M$の初期値を、ＯＩＤの全長Ｌと等しい長さで、かつ、すべての値が０であるビット列と定義する。また、変数$ＯＩＤ_V$の初期値を、ＯＩＤの全長Ｌと等しい長さで、かつ、すべての値が０であるビット列と定義する（ステップＳ２５１１）。

【００９９】

２．処理対象のＡＩＤの集合から１個のＡＩＤを選択し、以下のビット演算を実

行する（ステップＳ２５１３）。

【０１００】

(a) ＡＩＤに含まれる位置情報をもとにして、変数$ＡＩＤ_{M}$と変数$ＡＩＤ_{V}$の値を決定する（ステップＳ２５１５）。ここで、

・$ＡＩＤ_{M}$はＯＩＤの全長Ｌと等しい長さで、かつ、

－ＯＩＤ情報が定義されている位置の値は１である。

－ＯＩＤ情報が定義されていない位置の値は０である。

ビット列と定義する（図２６）。

【０１０１】

・$ＡＩＤ_{V}$はＯＩＤの全長Ｌと等しい長さで、かつ、

－ＯＩＤ情報が定義されている位置の値はＯＩＤ情報の実際の値である

－ＯＩＤ情報が定義されていない位置の値は０である

ビット列と定義する（図２６）。

【０１０２】

(b) $ＯＩＤ_{M}$と$ＡＩＤ_{M}$のＡＮＤ演算を実行し、その結果を変数$ＯＶＲ_{M}$に代入する（ステップＳ２５１７）。

【０１０３】

(c) $ＯＶＲ_{M}$と$ＡＩＤ_{M}$のＡＮＤ演算と、$ＯＶＲ_{M}$と$ＯＩＤ_{M}$のＡＮＤ演算を実行し、その演算結果を比較する（ステップＳ２５１９）。

・一致する場合$ＯＩＤ_{M}$と$ＡＩＤ_{M}$のＯＲ演算を実行し、実行結果を$ＯＩＤ_{M}$に代入する（ステップＳ２５２１）。また、$ＯＩＤ_{V}$と$ＡＩＤ_{V}$のＯＲ演算を実行し、実行結果を$ＯＩＤ_{M}$に代入する（ステップＳ２５２３）。

・一致しない場合、ステップＳ２５２５に進み、実行する。

【０１０４】

(d) 処理対象のＡＩＤの集合から、次に処理するＡＩＤを抽出する。

・集合に少なくとも１個のＡＩＤが含まれている場合、ステップＳ２５１９を実行する。

・集合にＡＩＤが１個も含まれていない場合、ステップＳ２５２７に進む。

【０１０５】

(e) OID_M およびOID_V の値を出力する（ステップＳ２５２７）。

【０１０６】

最終的に得られたOID_M の値は、処理対象のＡＩＤの集合から復元できたＯＩＤ情報のすべての位置を表している。また、最終的に得られたOID_V の値は、処理対象のＡＩＤの集合から復元できたＯＩＤ情報のすべてを表している。つまり、OID_M とOID_V の値を用いると、

(a) OID_V の値を検索条件とすると、確率的にではあるがＯＩＤを求めることができる。

【０１０７】

(b) 上記検索の精度を、ＯＩＤ全長Ｌとの比OID_M Ｌで定量的に評価することができる。

【０１０８】

上述したように、本実施形態では、ユーザは、氏名、電話番号、電子メールアドレスといった情報を含む個人識別子ＯＩＤからこれらの情報を隠蔽した役割識別子ＡＩＤを作成すべく図７に示すような役割識別子ＡＩＤ請求メッセージを作成し、認証局ＣＡ１に送信すると、認証局ＣＡ１は、該メッセージを受け取って、役割識別子ＡＩＤを生成し、ユーザに交付する。

【０１０９】

ユーザは、この交付された役割識別子ＡＩＤおよび性別、年齢、趣味等の個人情報をアノニマス・ディレクトリ・サービスＡＤＳ７に送信し、アノニマス・ディレクトリ・サービスＡＤＳ７に役割識別子ＡＩＤと個人情報を登録する。このように登録された情報を検索する場合は、検索者は自己の役割識別子ＡＩＤと検索条件（性別、年齢、趣味等のプライバシー情報）をアノニマス・ディレクトリ・サービスＡＤＳ７に送信する。アノニマス・ディレクトリ・サービスＡＤＳ７は、これらの情報を受信すると、該検索条件にマッチした登録者の役割識別子ＡＩＤを抽出する。そして、アノニマス・ディレクトリ・サービスＡＤＳ７は、検索者の役割識別子ＡＩＤと検索条件にマッチした登録者の役割識別子ＡＩＤから個別化アクセスチケットＰＡＴを生成し、検索者に交付する。

【０１１０】

この個別化アクセスチケットＰＡＴには、図３（ｃ）に示すように発信者フラグ、移転制御フラグ、有効期限の値が設定されるが、この有効期限を着信者側で設定することにより、発信者からの接続を制限することができる。

【０１１１】

また、移転制御フラグの設定内容により発信者に番号通知させるか否かを、すなわち着信者が発信者ＡＩＤと実際の発信者を対応づけられるようにすることができるか否かを選択することができる。すなわち、移転制御フラグを１に設定した場合には、セキュア・コミュニケーション・サービスＳＣＳ５で移転制御が行われ、着信者は発信者ＡＩＤと実際の発信者を対応付けることができる（発信者番号通知）。また、該フラグを０に設定した場合は、移転制御は行われず、着信者は発信者ＡＩＤと実際の発信者を対応付けることはできない（発信者番号非通知）。

【０１１２】

また、個別化アクセスチケットＰＡＴで着信者を指定した呼を個別化アクセスチケットＰＡＴ内で定義した着信者役割識別子ＡＩＤまたは発信者役割識別子ＡＩＤに着信するように、通信網に対して接続要求をすることができる。更に、個別化アクセスチケットＰＡＴで指定した呼のうち、着信者が選択した個別化アクセスチケットＰＡＴの呼を着信拒否することができる。また更に、匿名性を悪用し複数の発信者役割識別子ＡＩＤで個人攻撃を繰り返す発信者への対処として、それら複数の発信者役割識別子ＡＩＤから個人識別子ＯＩＤの同一性を判定することができ、かつ、その個人識別子をある確率で取り出すことができる。

【０１１３】

【発明の効果】

以上説明したように、本発明によれば、ユーザに役割識別子を付与し、役割識別子とユーザに関する情報とを対にして他のユーザから閲覧可能に保持し、発信者は役割識別子とユーザに関する情報に基づいて着信者を役割識別子で指定し、この指定に基づいて発信者に対して発信者役割識別子、着信者役割識別子、発信者フラグ、移転制御フラグ、および有効期限を含む個別化アクセスチケットを発

行し、役割識別子、個別化アクセスチケット、および個別化アクセスチケットに対する電子署名を用いて、個別化アクセスチケットが改竄されていなくて、発信者役割識別子が個別化アクセスチケットに含まれ、および個別化アクセスチケットが有効期限内であるという３要件を検証し、検証結果がすべて正しい場合に限り、発信者からの接続要求を通信網の物理的な接続制御方式に変換する接続制御を行うので、ユーザの本当の識別子を隠蔽しつつ、ユーザの特性を表す情報を公開し、この情報に基づいて適切な通信を行うことができ、従来のような第三者からの攻撃等を的確に防止することができる。加えて、着信者が匿名性を悪用した発信者による攻撃を受けた場合には、その攻撃による着信者への被害を最小限に食い止めることができる。

【図面の簡単な説明】

【図１】

本発明において使用される役割識別子ＡＩＤ、個別化アクセスチケットＰＡＴを示す説明図である。

【図２】

本発明の一実施形態の全体構成図である。

【図３】

個人識別子ＯＩＤと役割識別子ＡＩＤの例を示している。

【図４】

ユーザが役割識別子ＡＩＤを認証局ＣＡに対して請求する処理を示すフローチャートである。

【図５】

役割識別子ＡＩＤの請求に対する認証局ＣＡが役割識別子ＡＩＤをユーザに対して交付する処理を示すフローチャートである。

【図６】

ユーザにおけるＡＩＤ交付処理を示すフローチャートである。

【図７】

役割識別子ＡＩＤの請求メッセージの例を示す図である。

【図８】

役割識別子ＡＩＤの交付メッセージの例を示す図である。

【図９】

認証局ＣＡにおける役割識別子ＡＩＤの生成処理を示すフローチャートである。

【図１０】

図９のＡＩＤ生成処理に関連する説明図である。

【図１１】

アノニマス・ディレクトリ・サービスＡＤＳにおける役割識別子ＡＩＤの登録と個別化アクセスチケットＰＡＴの交付の例を示す説明図である。

【図１２】

ＡＤＳにおいて個別化アクセスチケットＰＡＴを生成する場合の処理を示すフローチャートである。

【図１３】

図１２のＰＡＴ生成処理に関連する説明図である。

【図１４】

ＳＣＳにおけるメール転送制御を示すフローチャートである。

【図１５】

ＳＣＳにおける移転制御を示すフローチャートである。

【図１６】

ユーザにおける移転制御を示すフローチャートである。

【図１７】

ＳＣＳにおける移転制御を示すフローチャートである。

【図１８】

ＳＣＳにおける個別化アクセスチケットＰＡＴに対する接続制御を示すフローチャートである。

【図１９】

ＳＣＳにおけるメール返信処理を示すフローチャートである。

【図２０】

ユーザ間の電子メールの例を示す図である。

【図２１】

着信拒否された場合の電子メールの例を示す図である。

【図２２】

ユーザにおける着信拒否申請処理を示すフローチャートである。

【図２３】

ＳＣＳにおける着信拒否設定処理を示すフローチャートである。

【図２４】

着信拒否申請メッセージおよび着信拒否通知メッセージの例を示す図である。

【図２５】

役割識別子ＡＩＤについて個人識別子ＯＩＤの同一性を判定する処理を示すフローチャートである。

【図２６】

図２５に示す同一性判定処理に関連する役割識別子ＡＩＤおよび個人識別子ＯＩＤの例を示す図である。

【図２７】

アナログ公衆網における二重番号登録を示す説明図である。

【図２８】

アナログ公衆網における発信者番号通知を示す説明図である。

【図２９】

デジタル携帯網およびアナログ公衆網における着信拒否を示す説明図である。

【図３０】

匿名電子メールの説明図である。

【符号の説明】

１　認証局ＣＡ

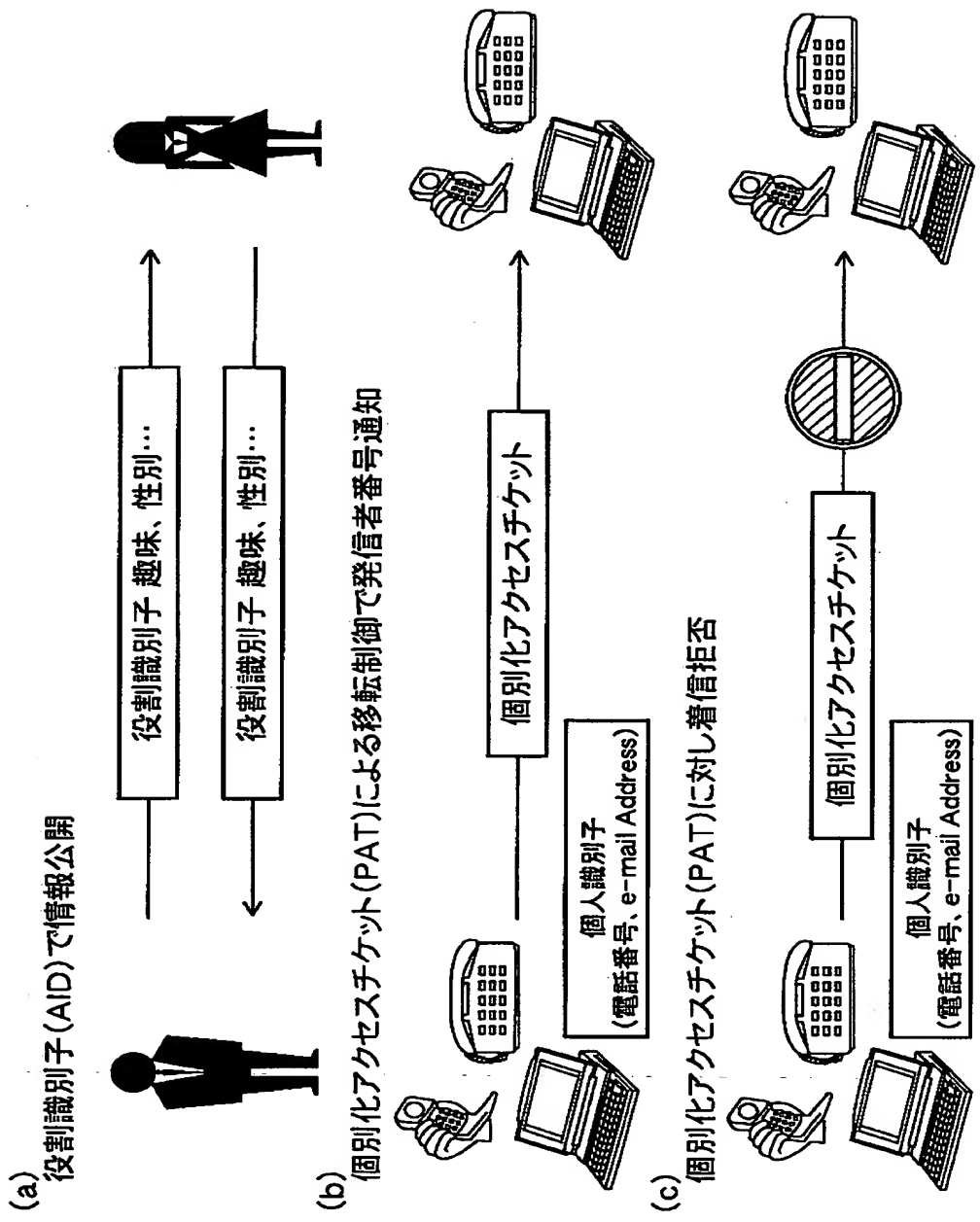
３　ユーザ

５　セキュア・コミュニケーション・サービスＳＣＳ

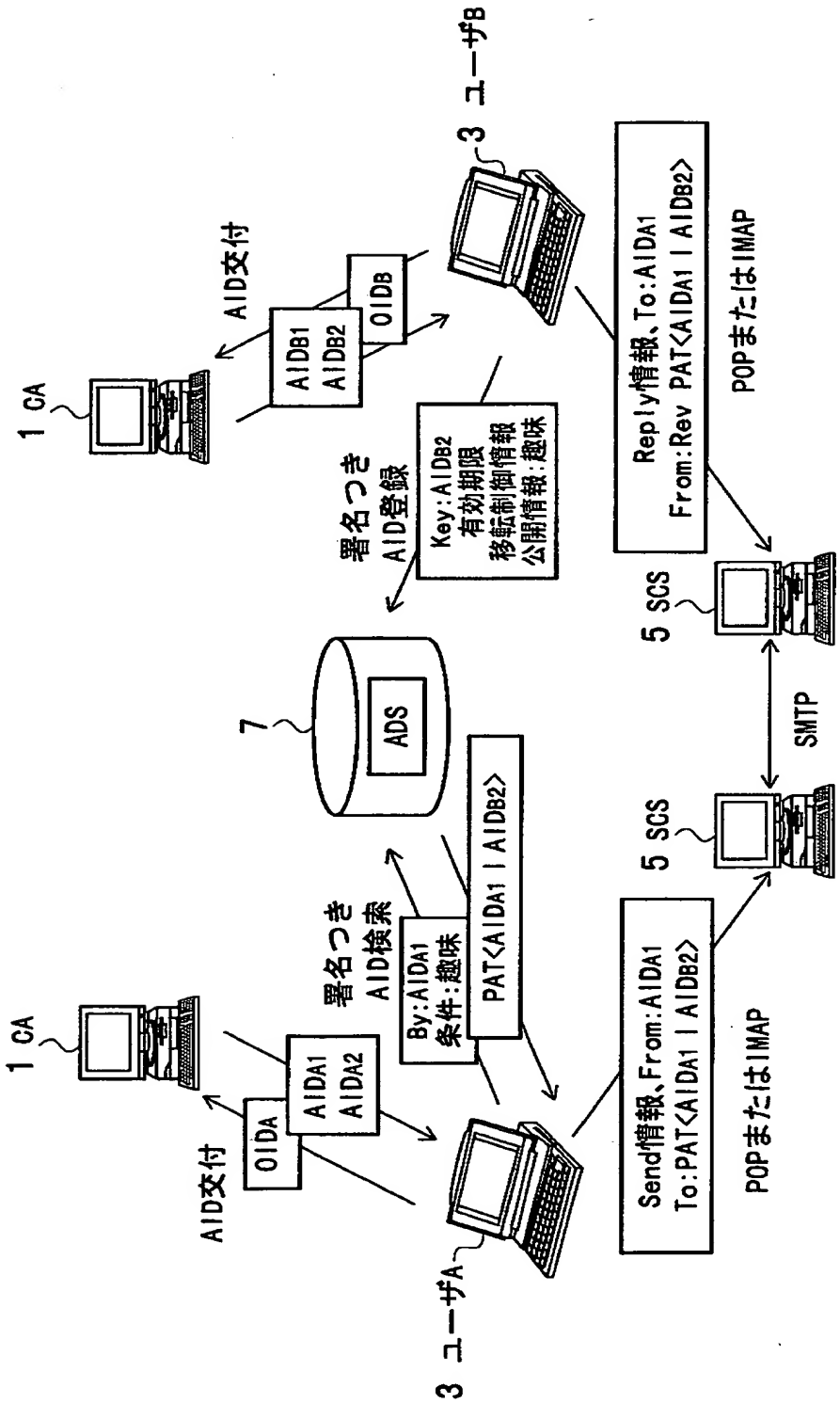
７　アノニマス・ディレクトリ・サービスＡＤＳ

【書類名】　　図面

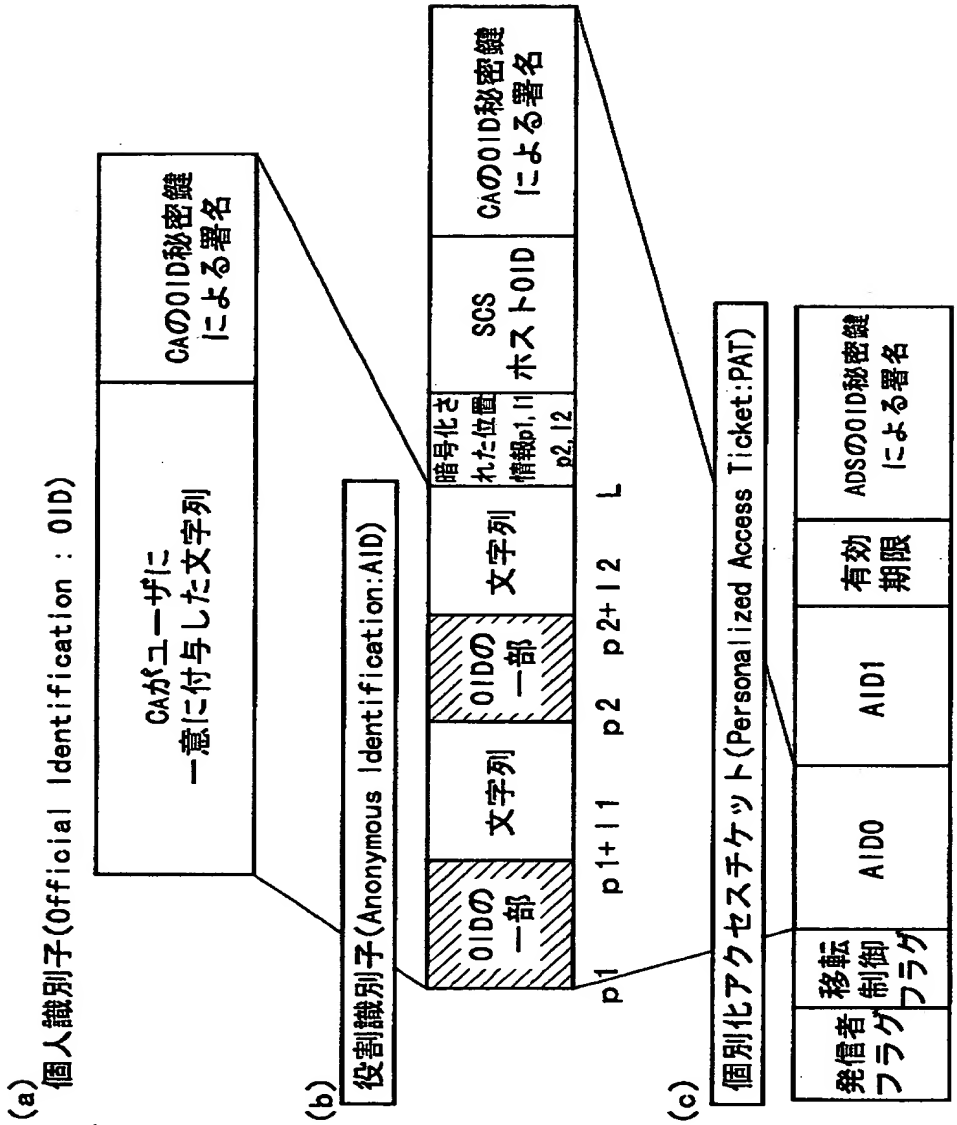
【図１】


(a)
役割識別子(AID)で情報公開
役割識別子 趣味、性別…
役割識別子 趣味、性別…
(b)
個別化アクセスチケット(PAT)による移転制御で発信者番号通知
個別化アクセスチケット
個人識別子
(電話番号、e-mail Address)
(c)
個別化アクセスチケット(PAT)に対し着信拒否
個別化アクセスチケット
個人識別子
(電話番号、e-mail Address)

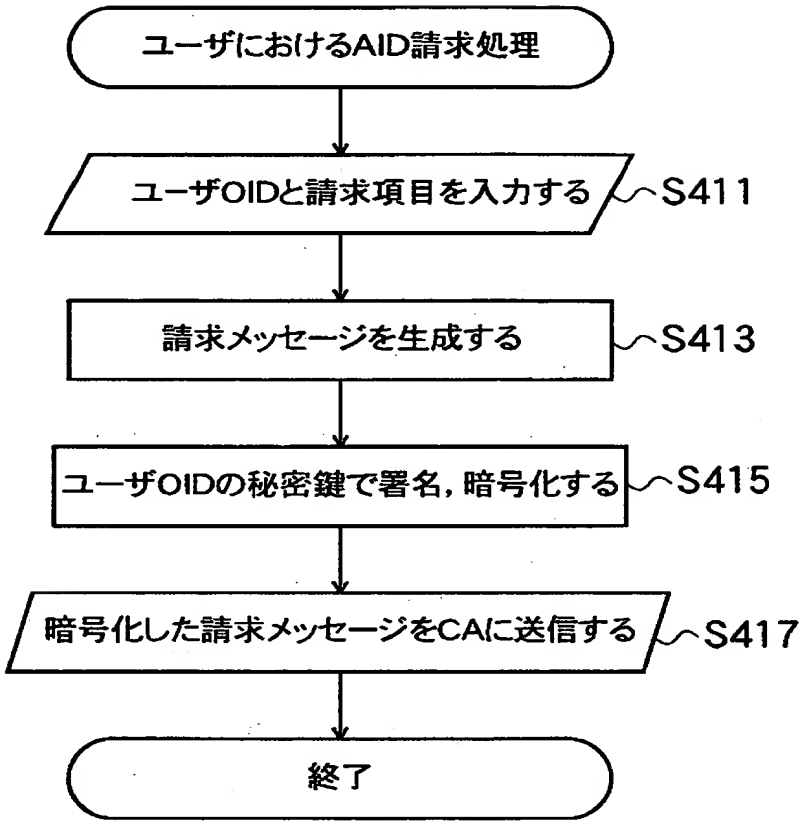
【図２】


1 CA
AID交付
AIDB1
AIDB2
OIDB
3 ユーザB
署名つき
AID登録
Key:AIDB2
有効期限
移転制御情報
公開情報:趣味
Reply情報、To:AIDA1
From:Rev PAT<AIDA1 | AIDB2>
POPまたはIMAP
5 SCS
SMTP
7
ADS
署名つき
AID検索
By:AIDA1
条件:趣味
PAT<AIDA1 | AIDB2>
Send情報、From:AIDA1
To:PAT<AIDA1 | AIDB2>
POPまたはIMAP
5 SGS
1 CA
AID交付
OIDA
AIDA1
AIDA2
3 ユーザA

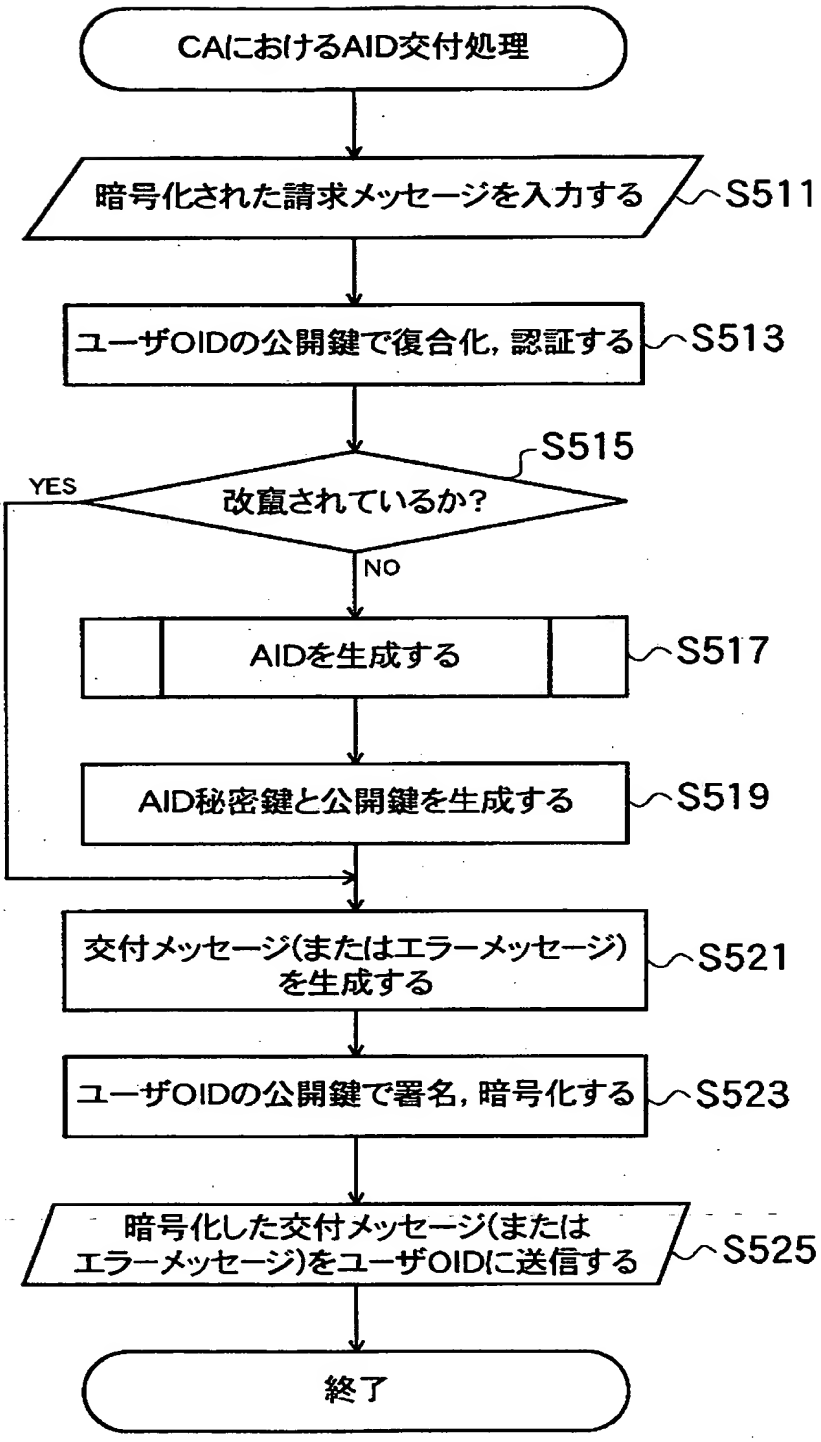
【図３】


(a)
個人識別子(Official Identification : OID)
CAがユーザに
一意に付与した文字列
CAのOID秘密鍵
による署名
(b)
役割識別子(Anonymous Identification:AID)
OIDの
一部
文字列
OIDの
一部
文字列
暗号化さ
れた位置
情報p1,l1
p2,l2
SCS
ホストOID
CAのOID秘密鍵
による署名
p1
p1+l1
p2
p2+l2
L
(c)
個別化アクセスチケット(Personalized Access Ticket:PAT)
発信者
フラグ
移転
制御
フラグ
AIDO
AID1
有効
期限
ADSのOID秘密鍵
による署名

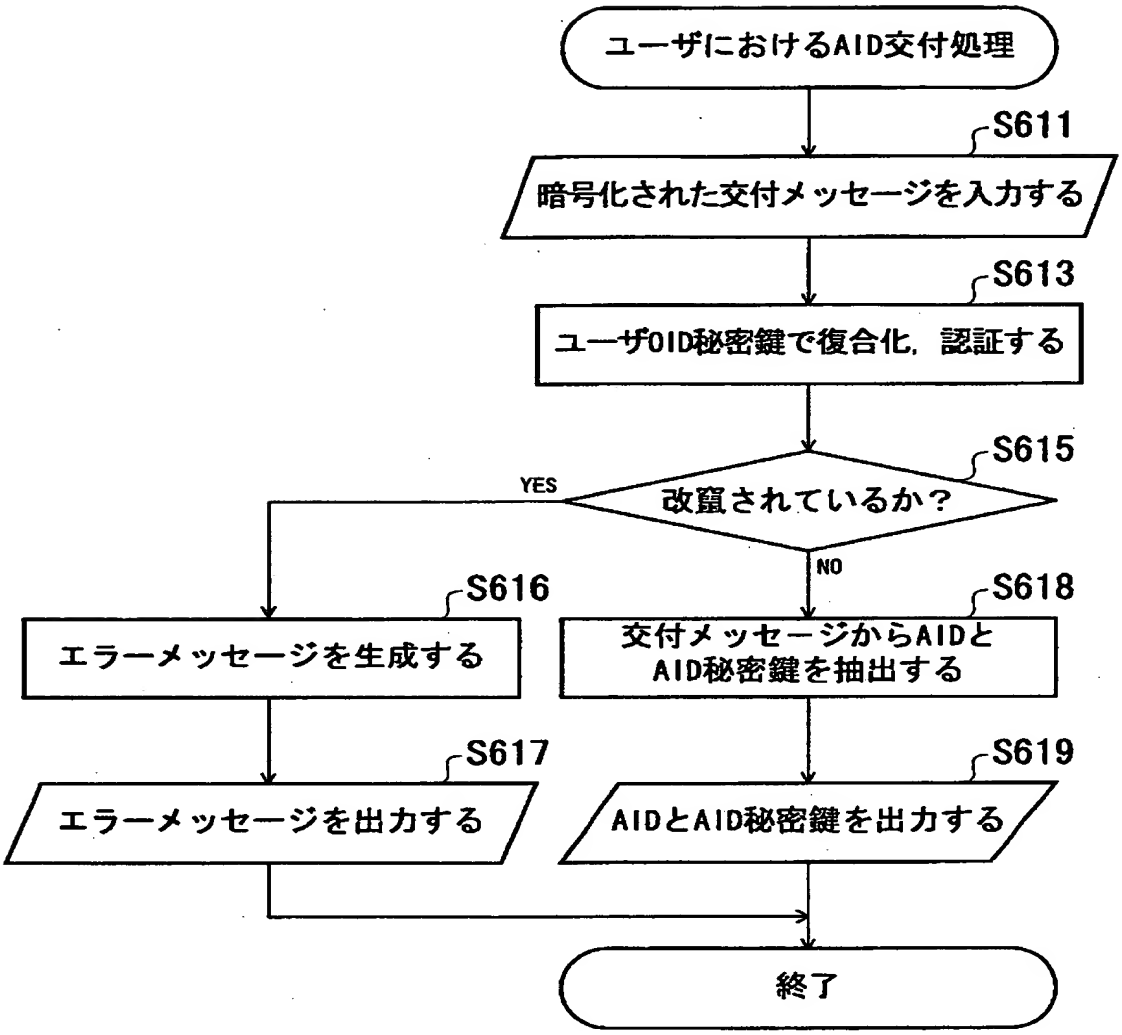
【図４】


ユーザにおけるAID請求処理
ユーザOIDと請求項目を入力する
S411
請求メッセージを生成する
S413
ユーザOIDの秘密鍵で署名，暗号化する
S415
暗号化した請求メッセージをCAに送信する
S417
終了

【図５】


CAにおけるAID交付処理
暗号化された請求メッセージを入力する
S511
ユーザOIDの公開鍵で復合化，認証する
S513
S515
YES
改竄されているか?
NO
AIDを生成する
S517
AID秘密鍵と公開鍵を生成する
S519
交付メッセージ(またはエラーメッセージ)を生成する
S521
ユーザOIDの公開鍵で署名，暗号化する
S523
暗号化した交付メッセージ(またはエラーメッセージ)をユーザOIDに送信する
S525
終了

【図６】


ユーザにおけるAID交付処理
S611
暗号化された交付メッセージを入力する
S613
ユーザOID秘密鍵で復合化，認証する
S615
改竄されているか？
YES
NO
S616
エラーメッセージを生成する
S618
交付メッセージからAIDと
AID秘密鍵を抽出する
S617
エラーメッセージを出力する
S619
AIDとAID秘密鍵を出力する
終了

【図７】

AID請求メッセージの例

REQUEST AID　2　　(新規AIDを2個請求する場合)

＜ユーザOIDの秘密鍵による署名＞
(送信時には，ユーザOIDの秘密鍵で暗号化する)

DISCARD AID AID1の実体　AID1の秘密鍵
DISCARD AID AID2の実体　AID2の秘密鍵
(既存AIDであるAID1とAID2を廃止したい場合)

＜ユーザOID秘密鍵による署名＞
(送信時には，ユーザOIDの秘密鍵で暗号化する)

【図８】

AID交付メッセージの例

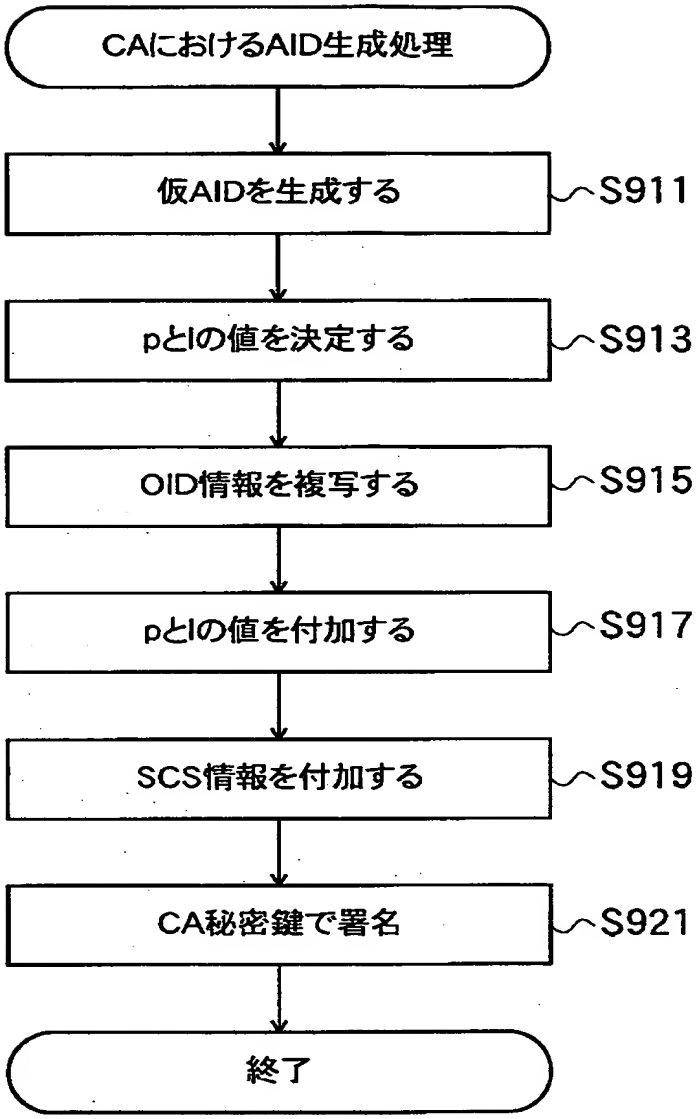
NEW AID AID3の実体　AID3の秘密鍵 OK
(新規AIDであるAID3は交付成功)
NEW AID NG　　(交付失敗,つまり,エラーメッセージ)

＜ユーザOIDの公開鍵による署名＞
(送信時には，ユーザOIDの公開鍵で暗号化する)

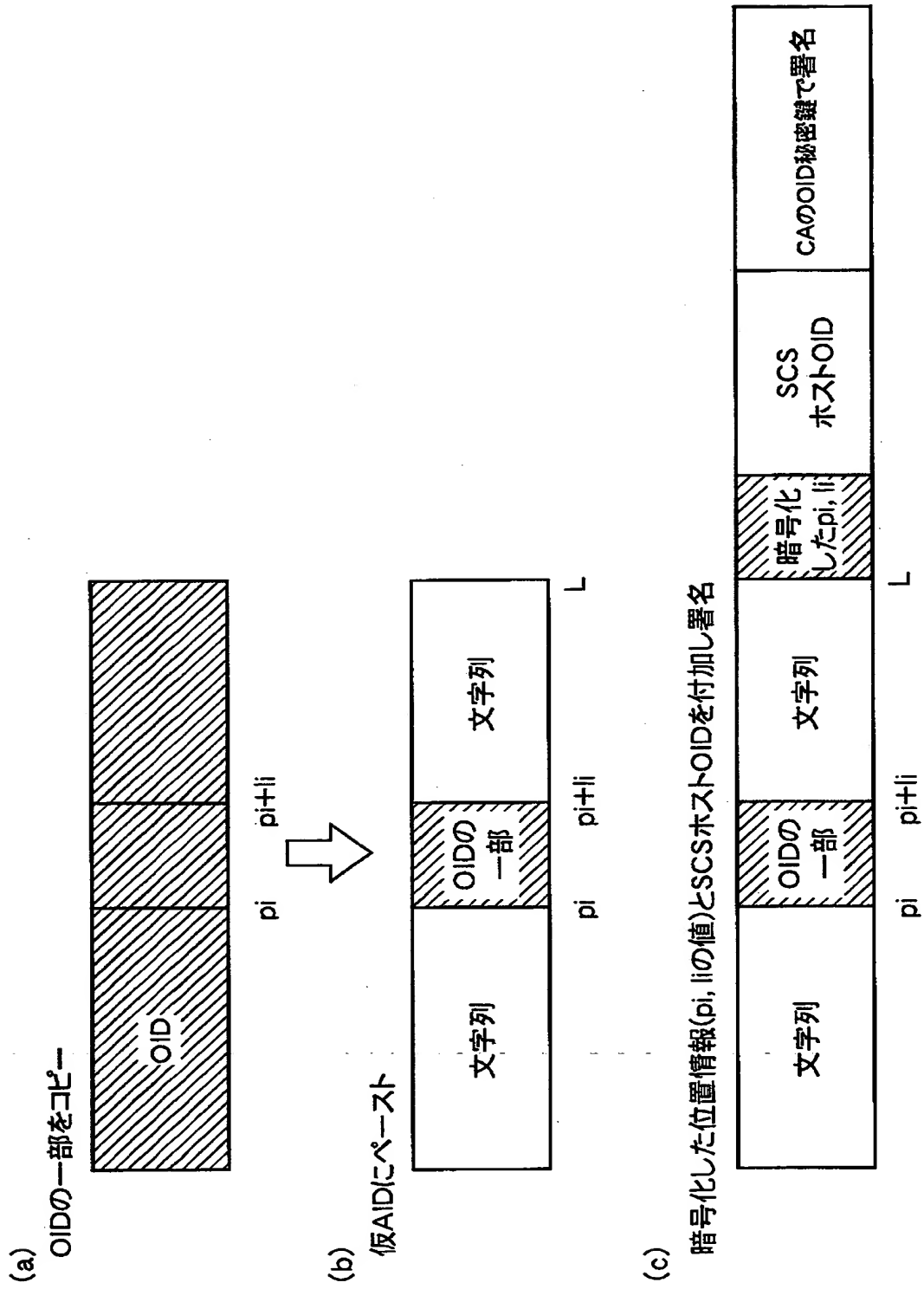
DISCARD AID AID1の実体 OK　　(既存AIDであるAID1は廃止成功)
DISCARD AID AID2の実体 NG
(既存AIDであるAID2の廃止失敗のエラーメッセージ)

＜ユーザOIDの公開鍵による署名＞
(送信時には，ユーザOIDの公開鍵で暗号化する)

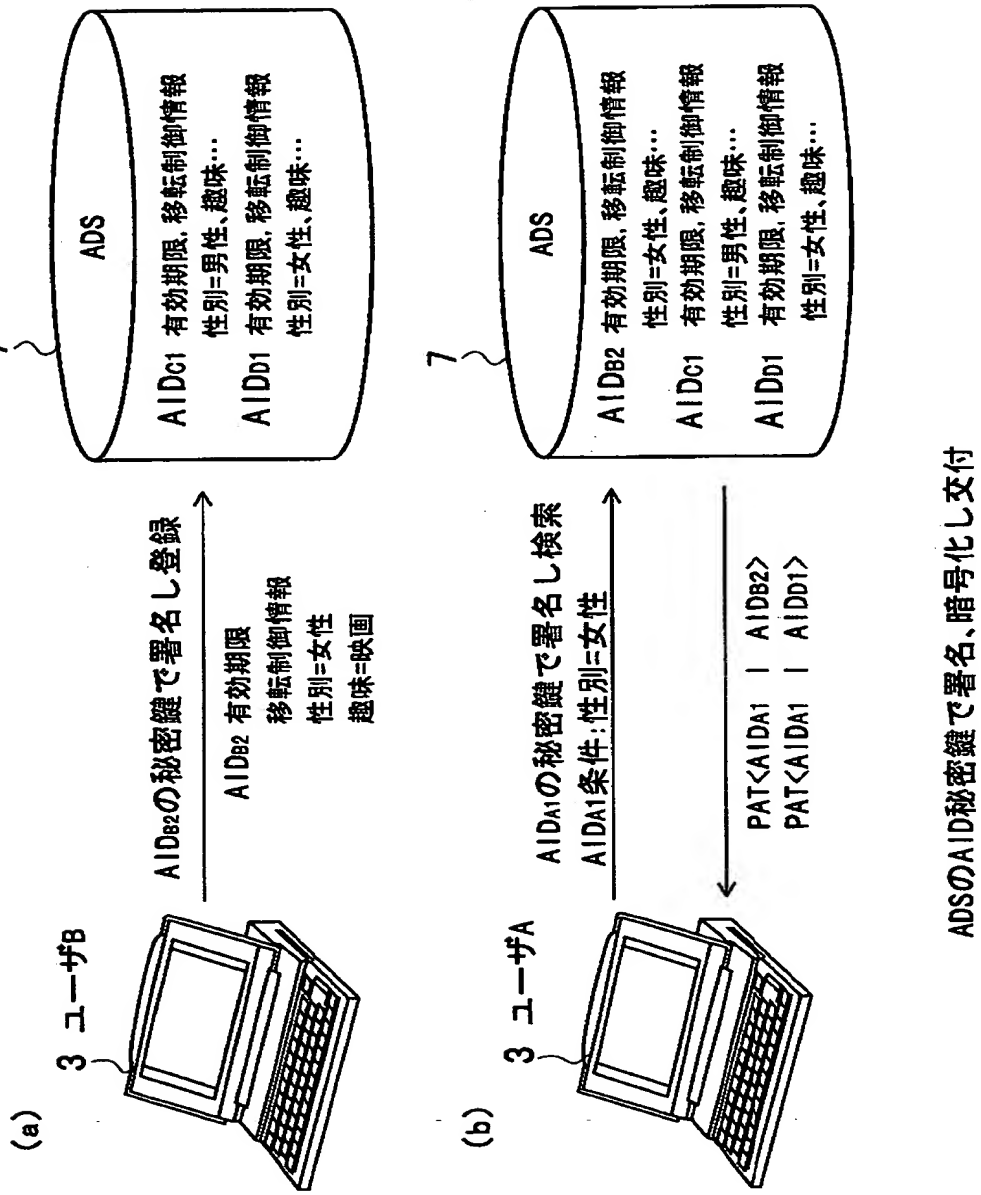
【図９】


CAにおけるAID生成処理
仮AIDを生成する
S911
pとlの値を決定する
S913
OID情報を複写する
S915
pとlの値を付加する
S917
SCS情報を付加する
S919
CA秘密鍵で署名
S921
終了

【図１０】

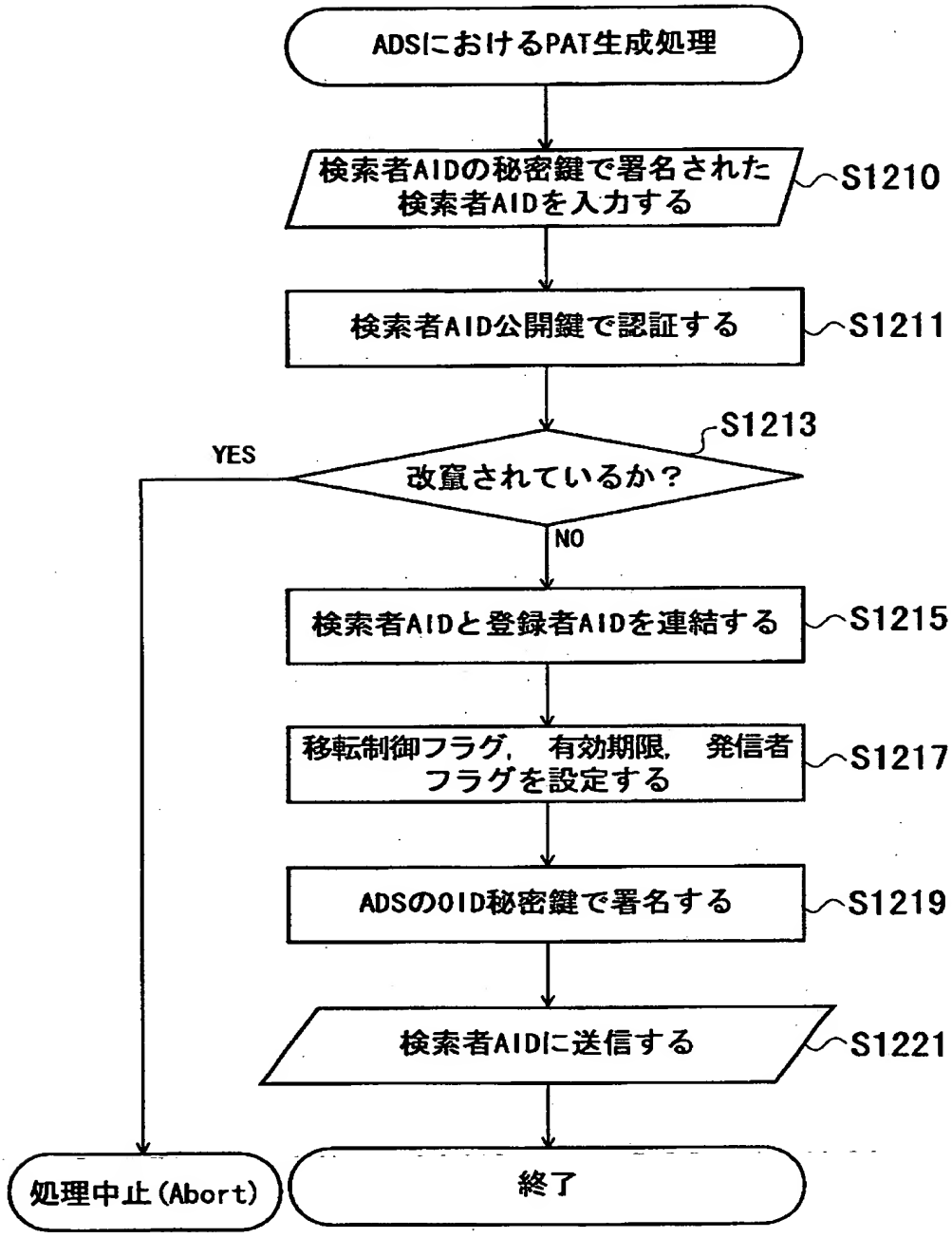

(a)
OIDの一部をコピー
OID
pi
pi+li
(b)
仮AIDにペースト
文字列
OIDの一部
文字列
L
pi
pi+li
(c)
暗号化した位置情報(pi, liの値)とSCSホストOIDを付加し署名
文字列
OIDの一部
文字列
暗号化したpi, li
SCSホストOID
CAのOID秘密鍵で署名
L
pi
pi+li

【図１１】

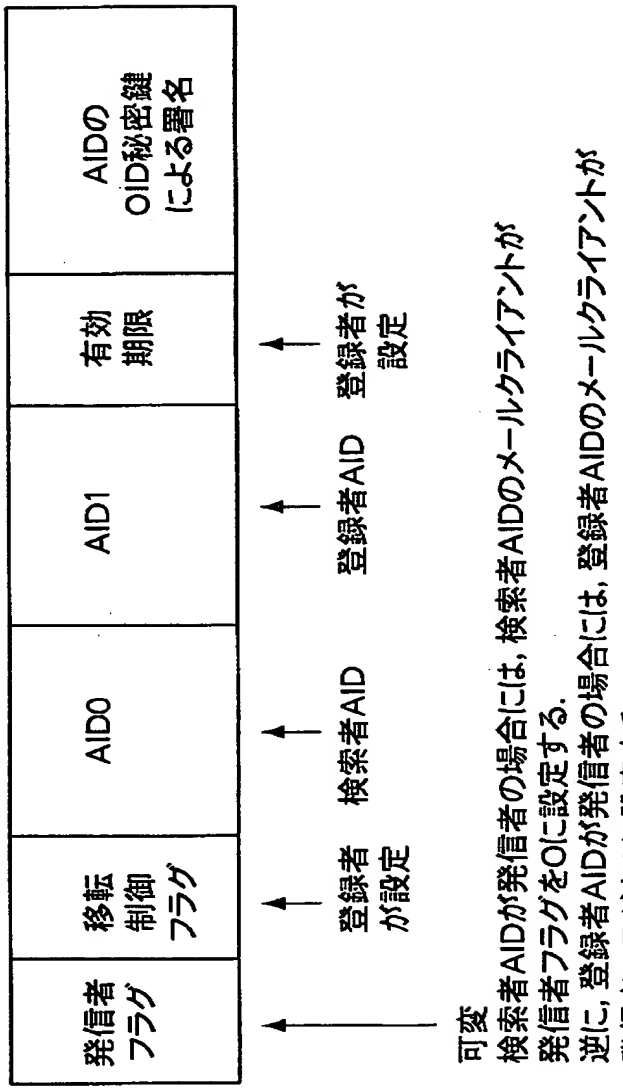


ADSのAID秘密鍵で署名、暗号化し交付

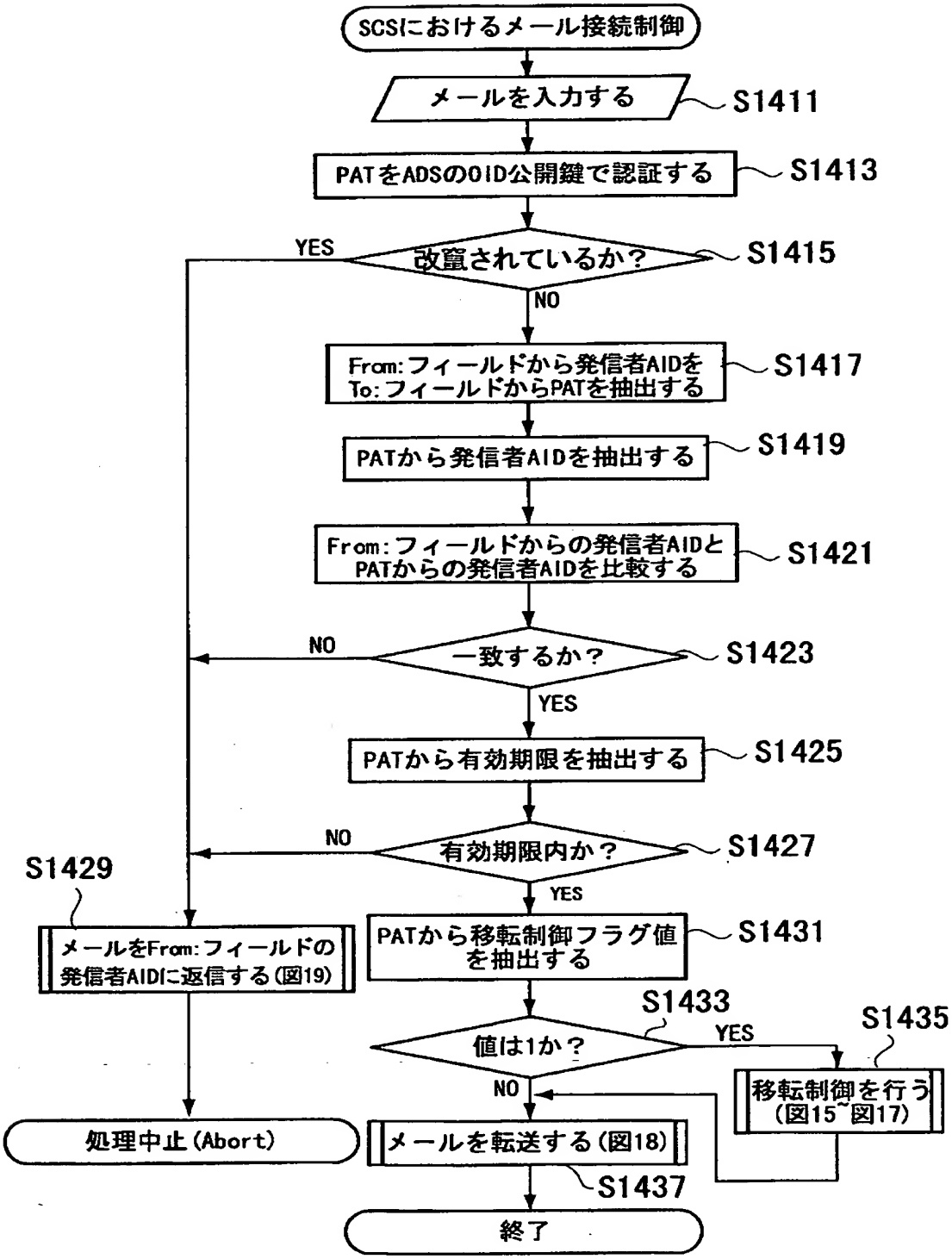
【図１２】


ADSにおけるPAT生成処理
検索者AIDの秘密鍵で署名された検索者AIDを入力する
S1210
検索者AID公開鍵で認証する
S1211
S1213
改竄されているか？
YES
NO
検索者AIDと登録者AIDを連結する
S1215
移転制御フラグ，有効期限，発信者フラグを設定する
S1217
ADSのOID秘密鍵で署名する
S1219
検索者AIDに送信する
S1221
処理中止(Abort)
終了

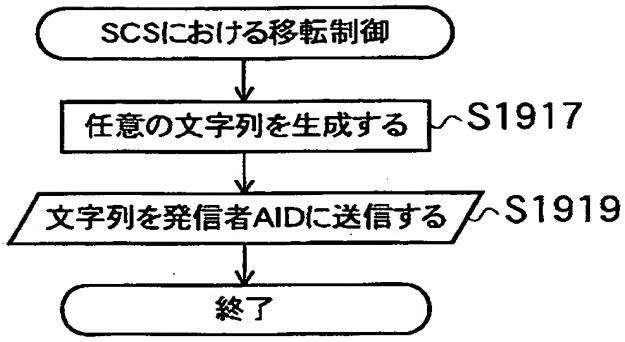
【図１３】


発信者フラグ
移転制御フラグ
AID0
AID1
有効期限
AIDのOID秘密鍵による署名
登録者が設定
検索者AID
登録者AID
登録者が設定
可変
検索者AIDが発信者の場合には，検索者AIDのメールクライアントが発信者フラグを0に設定する．
逆に，登録者AIDが発信者の場合には，登録者AIDのメールクライアントが発信者フラグを0に設定する．

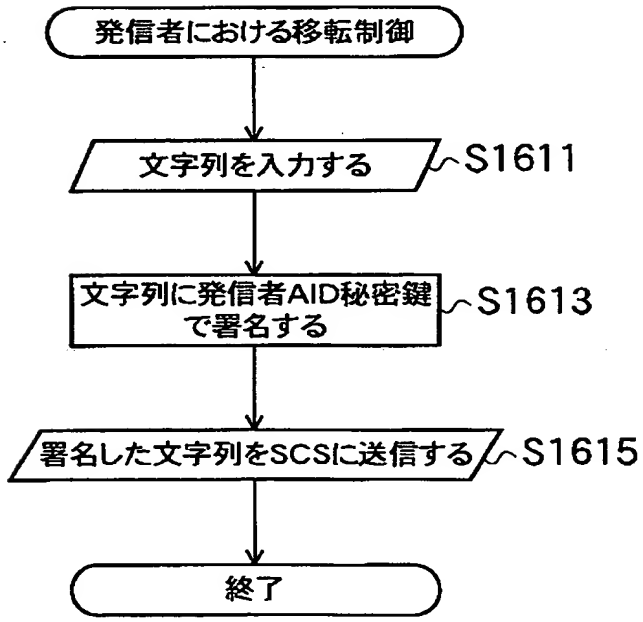
【図１４】


SCSにおけるメール接続制御
メールを入力する
S1411
PATをADSのOID公開鍵で認証する
S1413
YES
改竄されているか？
S1415
NO
From:フィールドから発信者AIDを
To:フィールドからPATを抽出する
S1417
PATから発信者AIDを抽出する
S1419
From:フィールドからの発信者AIDと
PATからの発信者AIDを比較する
S1421
NO
一致するか？
S1423
YES
PATから有効期限を抽出する
S1425
NO
有効期限内か？
S1427
YES
S1429
メールをFrom:フィールドの
発信者AIDに返信する(図19)
PATから移転制御フラグ値
を抽出する
S1431
S1433
値は1か？
YES
S1435
NO
移転制御を行う
(図15~図17)
処理中止(Abort)
メールを転送する(図18)
S1437
終了

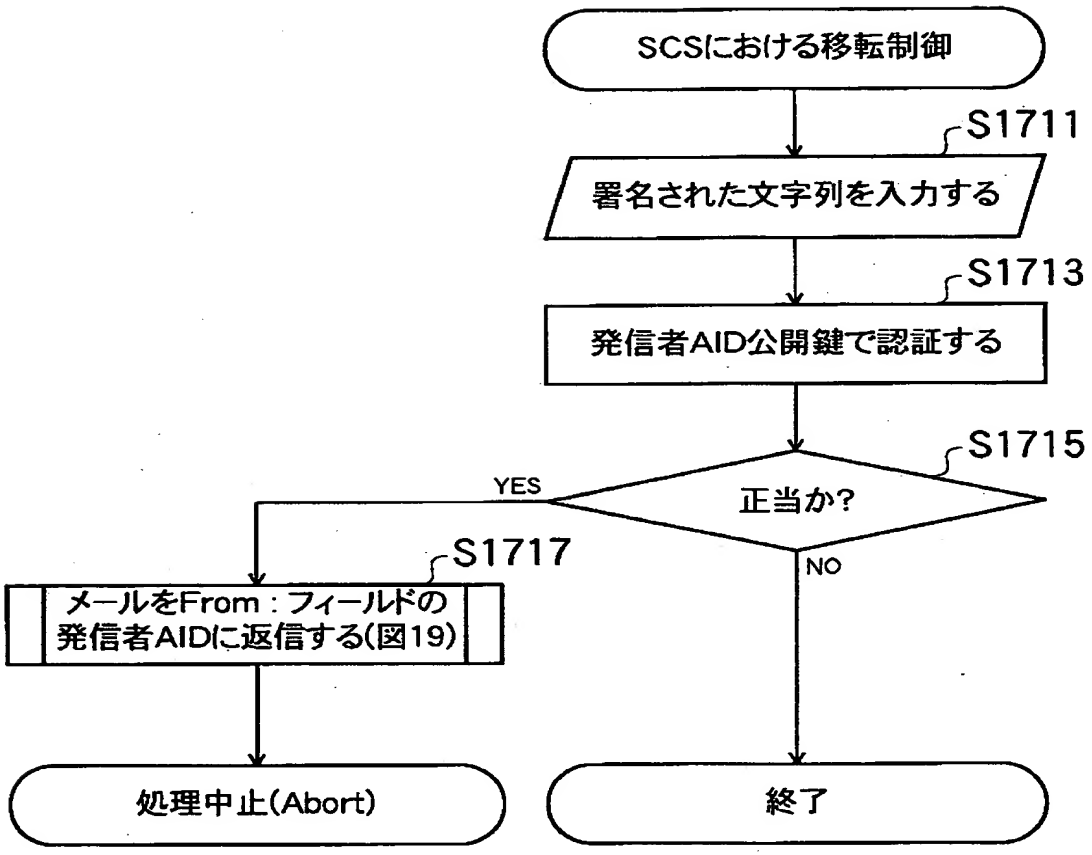
【図１５】


SCSにおける移転制御
任意の文字列を生成する
S1917
文字列を発信者AIDに送信する
S1919
終了

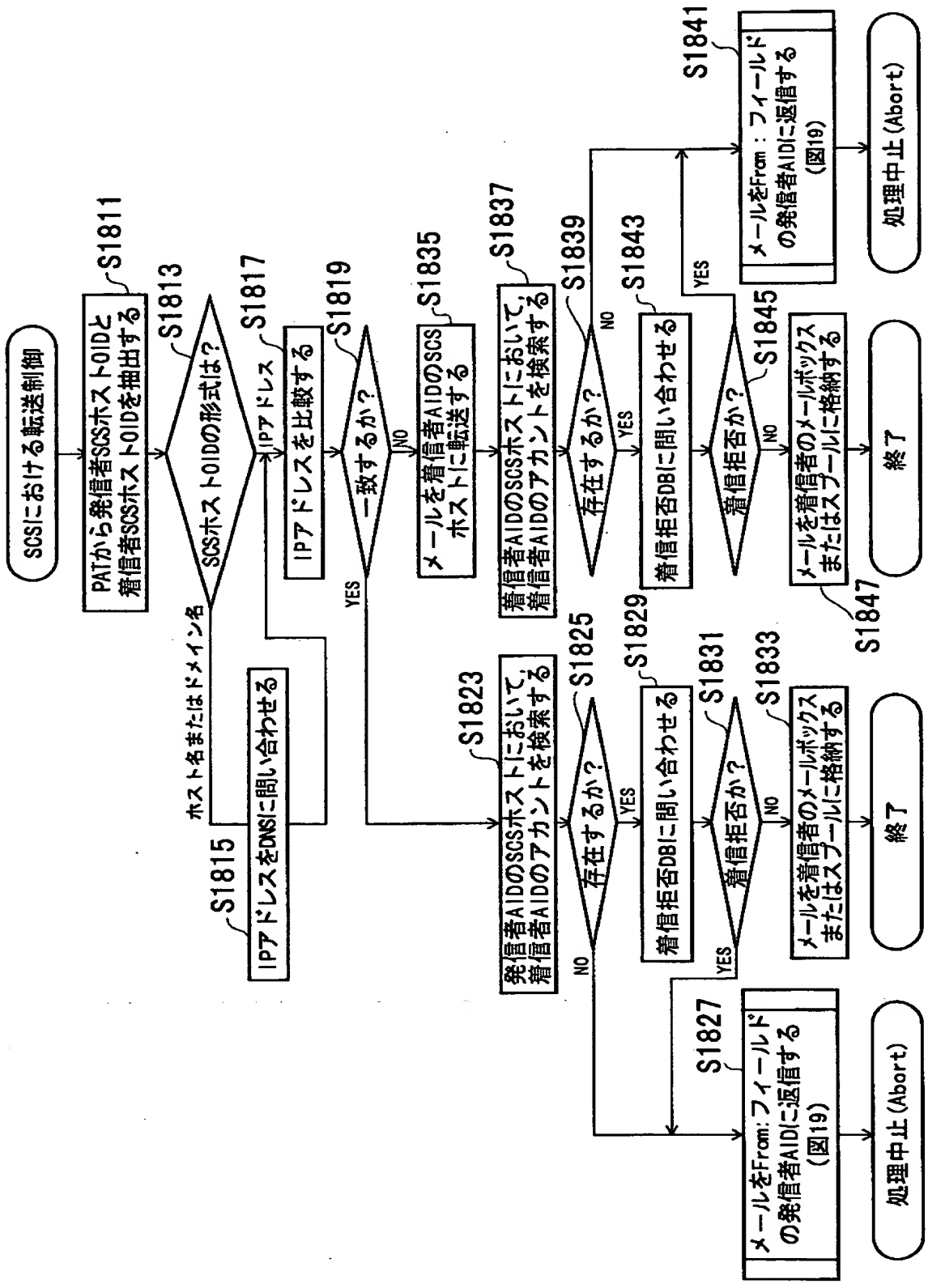
【図１６】


発信者における移転制御
文字列を入力する
S1611
文字列に発信者AID秘密鍵で署名する
S1613
署名した文字列をSCSに送信する
S1615
終了

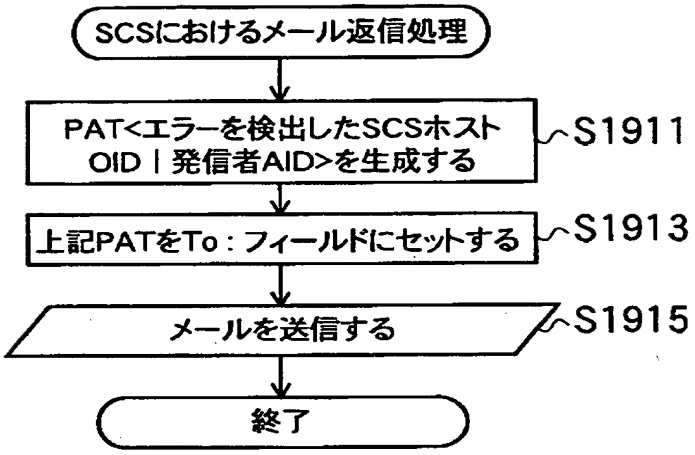
【図１７】


SCSにおける移転制御
S1711
署名された文字列を入力する
S1713
発信者AID公開鍵で認証する
S1715
正当か?
YES
NO
S1717
メールをFrom：フィールドの
発信者AIDに返信する(図19)
処理中止(Abort)
終了

【図１８】


SCSにおける転送制御
PATから発信者SCSホストOIDと着信者SCSホストOIDを抽出する
S1811
SCSホストOIDの形式は?
S1813
ホスト名またはドメイン名
IPアドレス
S1815
IPアドレスをDNSに問い合わせる
S1817
IPアドレスを比較する
S1819
一致するか?
YES
NO
メールを着信者AIDのSCSホストに転送する
S1835
着信者AIDのSCSホストにおいて,着信者AIDのアカントを検索する
S1837
存在するか?
S1839
NO
YES
着信拒否DBに問い合わせる
S1843
着信拒否か?
S1845
YES
NO
メールを着信者のメールボックスまたはスプールに格納する
S1847
メールをFrom:フィールドの発信者AIDに返信する(図19)
S1841
処理中止(Abort)
終了
発信者AIDのSCSホストにおいて,着信者AIDのアカントを検索する
S1823
存在するか?
S1825
NO
YES
着信拒否DBに問い合わせる
S1829
着信拒否か?
S1831
YES
NO
メールを着信者のメールボックスまたはスプールに格納する
S1833
メールをFrom:フィールドの発信者AIDに返信する(図19)
S1827
処理中止(Abort)
終了

【図１９】



【図２０】

クライアント間の電子メールの例

送信

From：<ユーザAのAID>
To：PAT<ユーザAのAID | ユーザBのAID>
Subject：こんにちわ

いい天気ですね.

返信

From：<ユーザBのAID>
To：Rev PAT<ユーザAのAID | ユーザBのAID>
Subject：Re：こんにちわ

そうですね.

PAT<A | B>は発信者フラグが0(つまり発信者はA)のPAT
Rev PAT<A | B>は発信者フラグが1(つまり発信者はB)のPAT

【図２１】

着信拒否された場合の電子メールの例

送信

From : <ユーザAのAID>
To : PAT<ユーザAのAID ! ユーザBのAID>
Subject : こんにちわ

いい天気ですね.

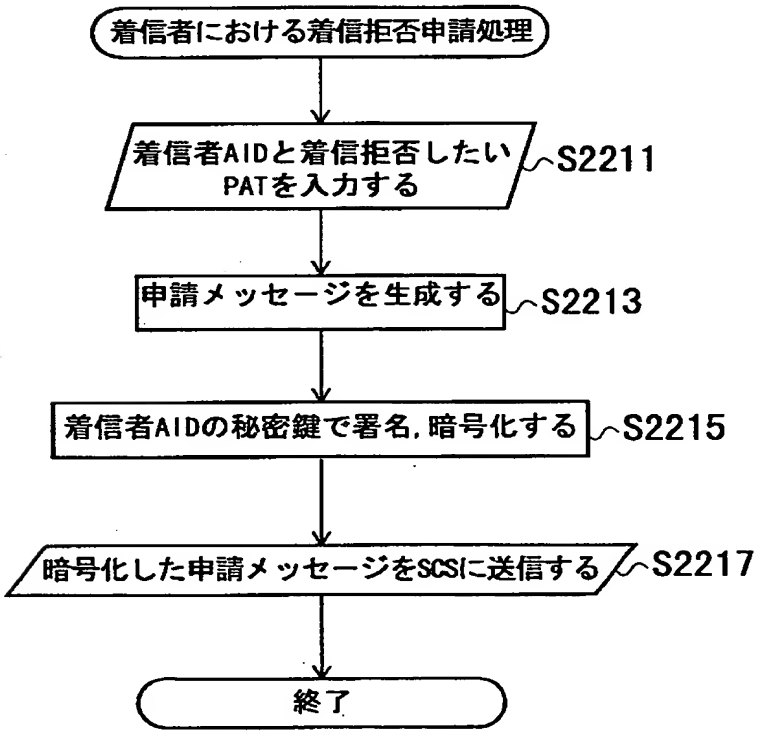
返信

From : <SCSのホストOID>
To : PAT<SCSのホストOID ! ユーザAのAID>
Subject : 着信拒否通知

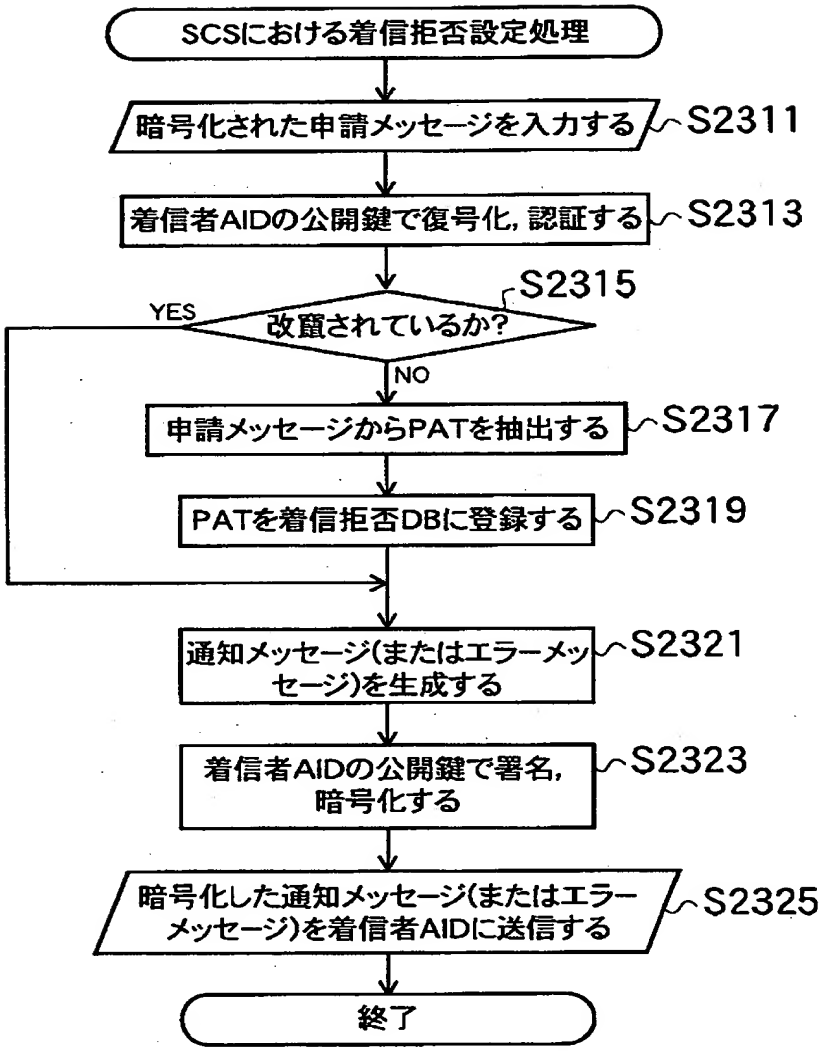
以下のメールは着信拒否されています.

>From : <ユーザAのAID>
>To : PAT<ユーザAのAID ! ユーザBのAID>
>Subject : こんにちわ
>
>いい天気ですね.

【図２２】



【図２３】


SCSにおける着信拒否設定処理
暗号化された申請メッセージを入力する
S2311
着信者AIDの公開鍵で復号化，認証する
S2313
S2315
YES
改竄されているか?
NO
申請メッセージからPATを抽出する
S2317
PATを着信拒否DBに登録する
S2319
通知メッセージ(またはエラーメッセージ)を生成する
S2321
着信者AIDの公開鍵で署名，暗号化する
S2323
暗号化した通知メッセージ(またはエラーメッセージ)を着信者AIDに送信する
S2325
終了

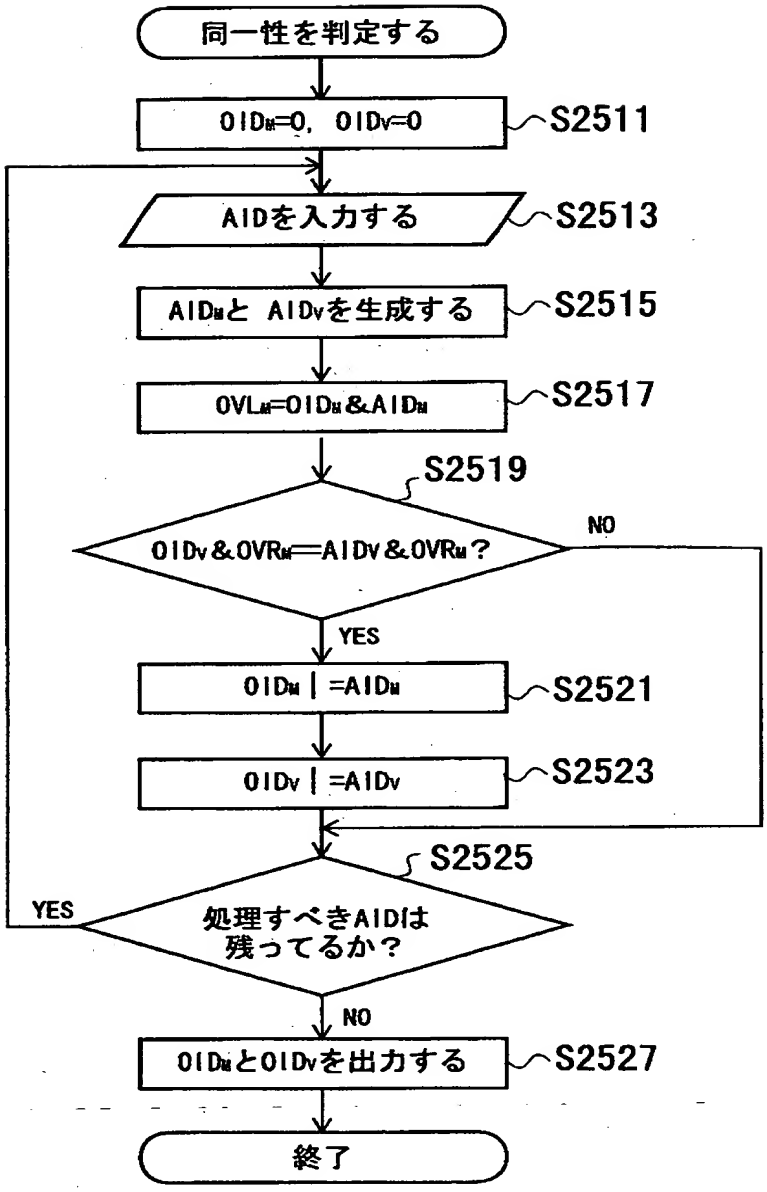
【図２４】

着信拒否申請・通知メッセージの例

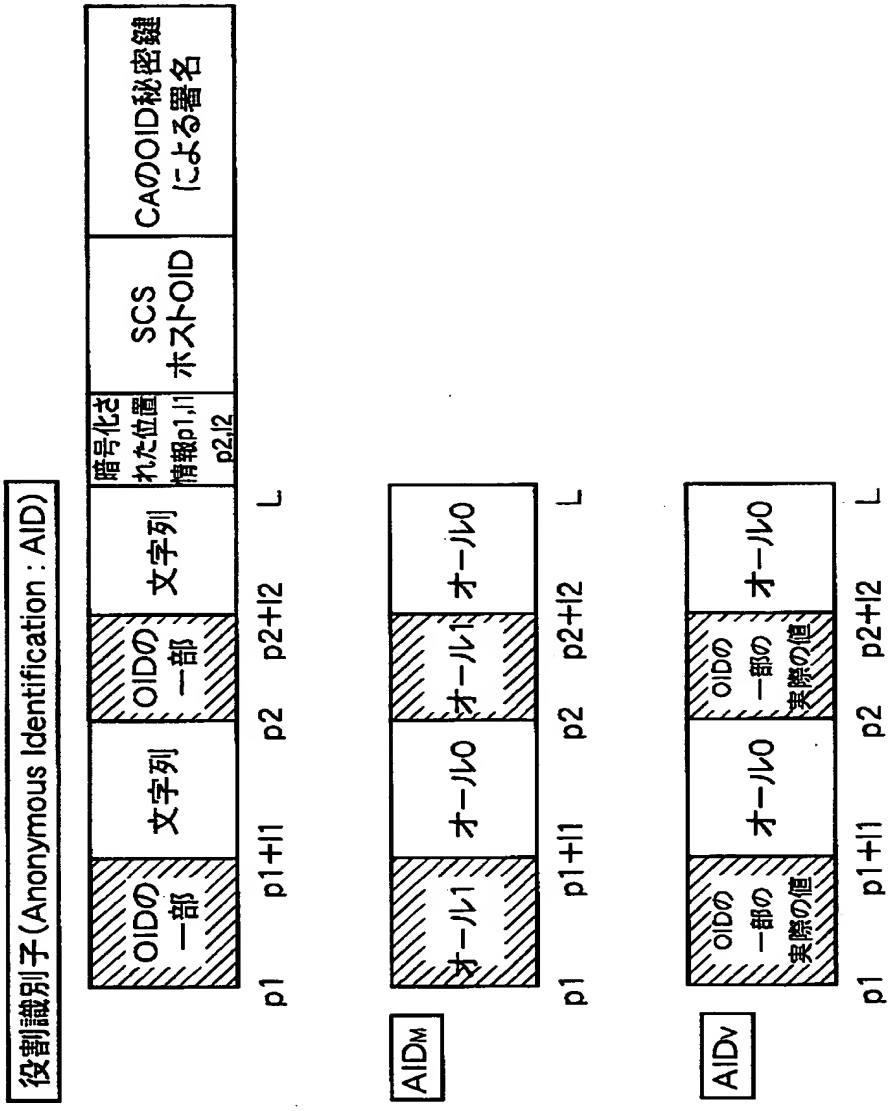
AIDの実体 REFUSE	PAT, IPアドレス, ホスト名, ドメイン名の実体 (着信拒否の設定の場合)
AIDの実体 RECONNECT	PAT, IPアドレス, ホスト名, ドメイン名の実体 (着信拒否の解除の場合)
<着信者AIDの秘密鍵による署名>	

AIDの実体 REFUSE	OKPAT, IPアドレス, ホスト名, ドメイン名の実体 (設定成功の場合)
AIDの実体 RECONNECT	NGPAT, IPアドレス, ホスト名, ドメイン名の実体 (解除失敗の場合, つまり, エラーメッセージ)
<着信者AIDの公開鍵による署名>	

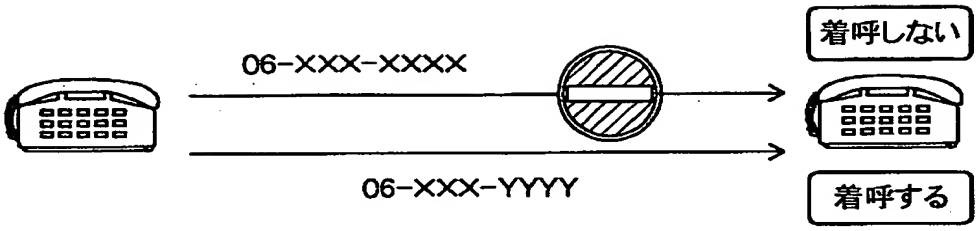
【図２５】


同一性を判定する
OIDM=0, OIDV=0
S2511
AIDを入力する
S2513
AIDMと AIDVを生成する
S2515
OVLM=OIDM&AIDM
S2517
S2519
OIDV&OVRM=AIDV&OVRM？
NO
YES
OIDM |=AIDM
S2521
OIDV |=AIDV
S2523
S2525
YES
処理すべきAIDは
残ってるか？
NO
OIDMとOIDVを出力する
S2527
終了

【図２６】

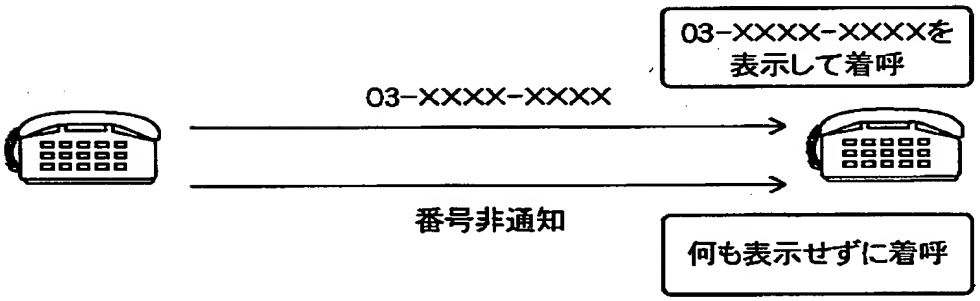

役割識別子(Anonymous Identification : AID)
OIDの一部
文字列
OIDの一部
文字列
暗号化された位置情報p1,l1 p2,l2
SCSホストOID
CAのOID秘密鍵による署名
p1
p1+l1
p2
p2+l2
L
AIDM
オール1
オール0
オール1
オール0
AIDV
OIDの一部の実際の値
オール0
OIDの一部の実際の値
オール0

【図２７】



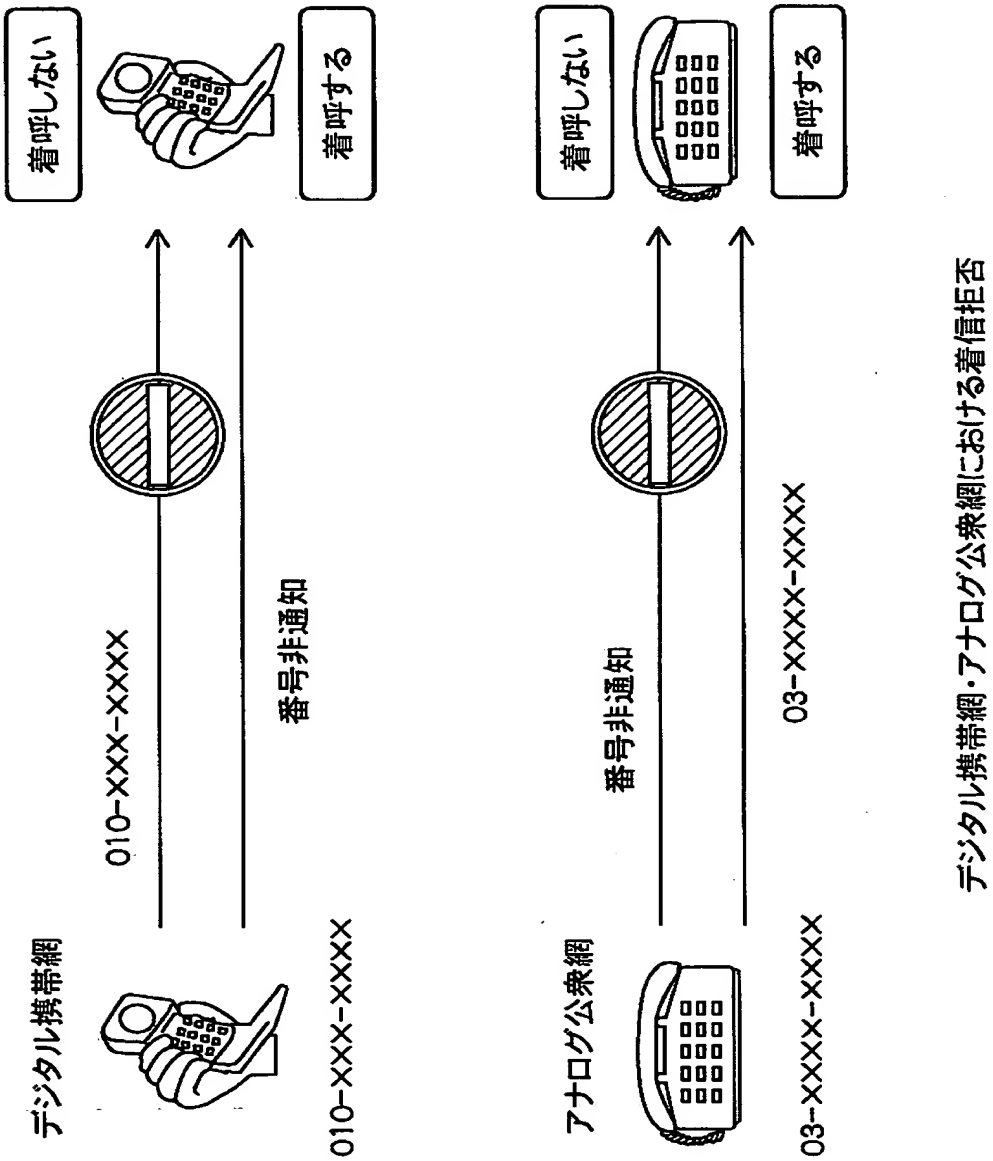
アナログ公衆網における二重番号登録

【図２８】

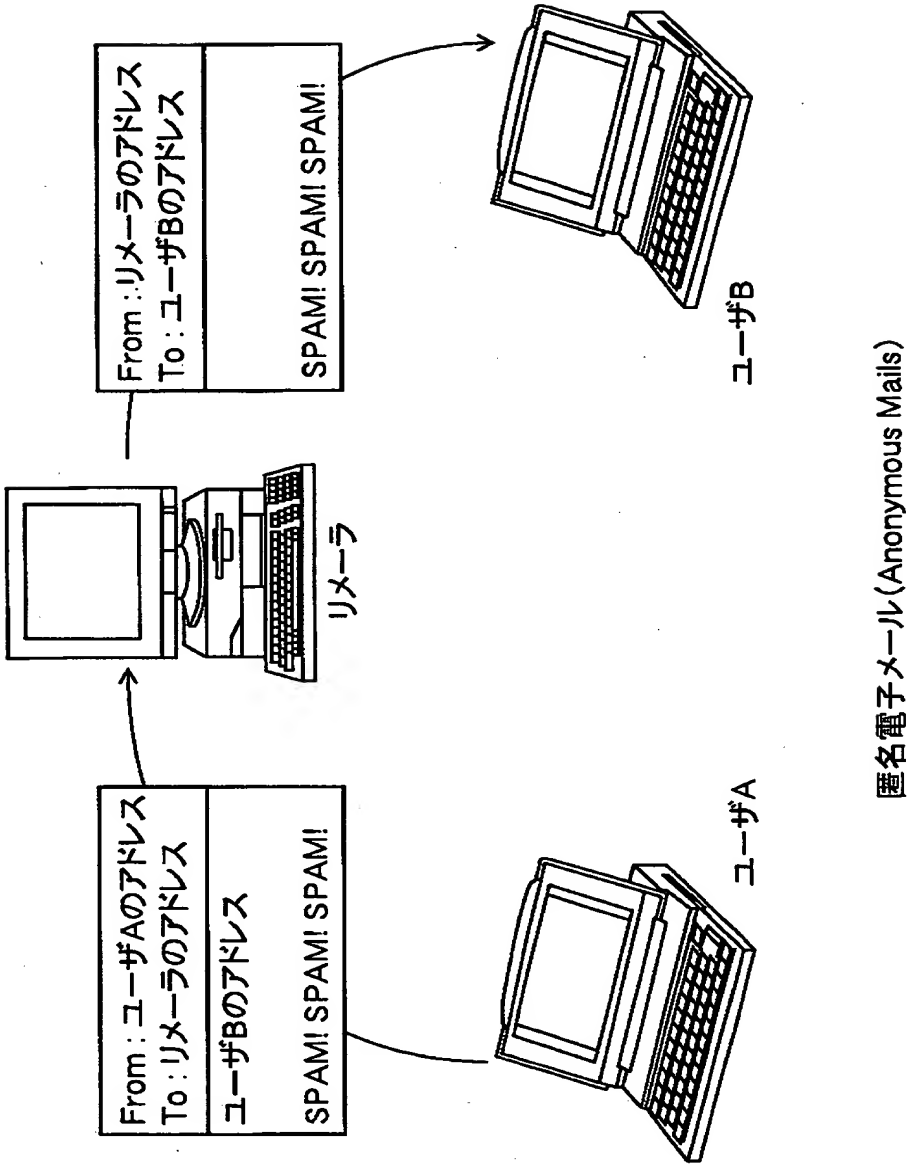


アナログ公衆網における発信者番号通知

【図２９】


着呼しない
着呼する
デジタル携帯網
010-XXX-XXXX
番号非通知
010-XXX-XXXX
アナログ公衆網
番号非通知
03-XXXX-XXXX
03-XXXX-XXXX
デジタル携帯網・アナログ公衆網における着信拒否

【図３０】


From：ユーザAのアドレス
To：リメーラのアドレス
ユーザBのアドレス
SPAM! SPAM! SPAM!
From：リメーラのアドレス
To：ユーザBのアドレス
SPAM! SPAM! SPAM!
リメーラ
ユーザA
ユーザB
匿名電子メール(Anonymous Mails)

【書類名】　　要約書

【要約】

【課題】　匿名性とセキュリティを確保すべく着信者の匿名性を保持しつつ発信者からの通信の接続を可能とする接続制御方法および通信網を提供する。

【解決手段】　ユーザに役割識別子を付与し、役割識別子とユーザに関する情報を閲覧可能に保持し、発信者は着信者を役割識別子で指定し、この指定に基づき発信者に発信者フラグ、移転制御フラグ、有効期限を含む個別化アクセスチケットを発行し、役割識別子と個別化アクセスチケットを用いて個別化アクセスチケットが有効期限内で正当であり、発信者役割識別子が個別化アクセスチケットに含まれ、着信者役割識別子が個別化アクセスチケットに含まれていることを検証し、検証結果がすべて正しい場合に発信者からの接続要求を通信網に物理的な接続制御方式に変換する接続制御を行う。

【選択図】　　図１

【書類名】　職権訂正データ
【訂正書類】　特許願

＜認定情報・付加情報＞
【特許出願人】
【識別番号】　000004226
【住所又は居所】　東京都新宿区西新宿三丁目１９番２号
【氏名又は名称】　日本電信電話株式会社
【代理人】　申請人
【識別番号】　100083806
【住所又は居所】　東京都港区虎ノ門１丁目２番３号　虎ノ門第一ビル９階　三好内外国特許事務所
【氏名又は名称】　三好　秀和
【選任した代理人】
【識別番号】　100068342
【住所又は居所】　東京都港区虎ノ門１丁目２番３号　虎ノ門第一ビル９階　三好内外国特許事務所
【氏名又は名称】　三好　保男

出　願　人　履　歴　情　報

識別番号　　〔０００００４２２６〕

１．変更年月日　　１９９５年　９月２１日
［変更理由］　住所変更
住　所　　東京都新宿区西新宿三丁目１９番２号
氏　名　　日本電信電話株式会社